DRPG

ACCEPTABLE USE GUIDELINES

Version:	1
Published:	24/01/2022
Created by:	James Hurley
Approved by:	Richard Parmenter
Confidentiality level:	Restricted

Contents

1 Purpose and scope

This policy applies to all **DRPG** team members who are offered access to company assets. It sets out what **DRPG** considers to be the acceptable use of those assets.

'Team Members' include all employees of **DRPG** as well as contractors, freelancers, temporary staff, apprentices, and third parties that are granted access to organisation information assets and who have had prior approval from the Information Security Manager.

2 Responsibilities and applicability

The Information Security Manager is responsible for ensuring this policy is up to date and reviewed annually

3 Referenced documents

ISO27001:2013 A.8.1.3

4 Introduction

The purpose of this policy is to ensure that the team members of **DRPG** understand the way in which IT, specifically ***Email***, ***Internet*** and ***social media***, should be used within the company.

Use of these facilities provided by **DRPG** team members is permitted and encouraged where such use is suitable for business purposes and supports the goals and objectives of the company. The internet is an unregulated environment and **DRPG** will not be liable for any material viewed or downloaded. Use of the Internet must be consistent with the **DRPG's** standards of business conduct as laid out in the 'Employee Handbook' and must occur as part of the normal execution of the team members job responsibilities. Any breach of the Acceptable Use Policy (the AUP) may lead to disciplinary action and possible termination of employment. Illegal activities will not be tolerated and may also be reported to the appropriate authorities.

5 Acceptable Use

5.1 **DRPG** User IDs, websites and e-mail accounts may only be used for **DRPG** sanctioned communications.

5.2 The distribution of any information through the Internet (including by e-mail, instant messaging systems and any other computer-based systems) may be scrutinised by **DRPG** and **DRPG** reserves the right to determine the suitability of the information.

5.3 The use of **DRPG** computer resources is subject to UK law (Data Protection, Computer Misuse Act etc), and any abuse will be dealt with appropriately.

6 Internet Acceptable Use

6.1 Team members may not visit Internet sites that contain pornography, obscene, hateful or other objectionable material, shall not attempt to bypass organisational web control technologies (Watchguard & Sophos Endpoint Protection) and shall not make or post indecent remarks, proposals or materials on the Internet or via Social Media sites.

6.2 Team members may not upload, download, or otherwise transmit commercial software or any copyrighted materials belonging to the company or any third parties, may not reveal or publicise confidential information.

6.3 Team members may not download software from the Internet or execute or accept any software programs or other code on the Internet unless it is in accordance with **DRPG**'s software policies and procedures and subject to authorisation from the IT Dept.

6.4 Team members will not carry out any other inappropriate internet activity as identified from time to time by **DRPG** and will not waste time or resources on non-organisation business.

This may include excessive use of and is not limited to downloading bandwidth intensive content such as streaming video, internet radio, torrents, MP3 music files and the sharing thereof.

7 Email Acceptable Use

7.1 Team members shall not solicit e-mails that are unrelated to business activity or which are for personal gain, shall not send or receive any material which is obscene or defamatory or which is intended to annoy, harass, or intimidate another person, and shall not present personal opinions/views as those of the company.

7.2 Organisational e-mail facilities may not be used for sending defamatory e-mails, or using e-mail for harassment, unauthorised purchases, or for publishing views and opinions (defamatory or otherwise) about team members, workers, suppliers, partners or clients of DRPG

7.3 All external bound e-mails will have an automatic footer that contains the legal disclaimer and team members are prohibited from amending or deleting it.

7.4 **DRPG** e-mail, may only be used for the communication of confidential information as long as it is in line with the requirements of ISMS DOC 8.2.

7.5 Outgoing e-mail attachments must be appropriately protected where required, using cryptographic controls such as Egress for information classification types.

7.6 Team members must not open incoming e-mail attachments that originate with unknown third parties or that, even if they appear to have been sent by a known party, were not expected. These attachments may contain viruses, worms or Trojans and any such e-mails must be reported to the Information Security Manager, by telephone, by email; to support@drpgroup.com or in person, and should only be forwarded to support for analysis.

7.7 Viruses and hoax virus messages: users are required to report any third-party e-mail messages they receive about viruses to the Information Security Manager immediately, by telephone, by email to support@drpgroup.com or in person, and on no account should it be forwarded, or copied on to anyone, whether inside or outside the network.

7.7 Team members are prohibited from using organisational e-mail facilities for forwarding chain letters or impersonating other people, nor may organisational e-mail addresses be left on any websites other than for legitimate and necessary business purposes.

7.8 Team members are requested to limit the use of group e-mail addresses, limit copying in unnecessary recipients.

7.9 Team members requiring to email the entire company may do so to all@drpgroup.com but the messages are subject to approval.

7.10 Team members are required to comply with the Incident Reporting Procedure in the event of any Information Security related breaches.

7.11 All incoming and outgoing DRPG email is archived with GFI MailArchiver. This is an email storage management system and is available to all team members upon request for backup/recovery purposes.

7.12 Team members are required to delete non-essential e-mail messages as soon as possible and, on a regular basis, to clear e-mail boxes of correspondence that is no longer required. The GFI Mail Archiver facility should be used so that messages that need to be retained but which are no longer current can be removed from the inbox or exported to a local PST folder. These controls are necessary so as to avoid e-mail boxes becoming so full that excessive server space is required to support the system. The sent items box must also be reviewed and cleared on a regular basis. The IT Manager will ensure that maximum individual mailbox sizes are set which, after two early automated warnings, cannot be exceeded.

7.13 Organisational e-mail may not be used to purchase anything on behalf of the drp without specific prior authorisation.

7.14 Team members are prohibited from setting up automatic forwarding of e-mails to addresses external to that of drp or of copying e-mails to addresses outside of drp unless there is a legitimate business purpose for doing so.

7.15 Breaches of these requirements may be dealt with under the DRPG disciplinary policy as set out in the Team Member Handbook.

8 Social Media Use

8.1 Blogging by team members, whether using **DRPG**'s property and systems or personal devices and computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of **DRPG**'s systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate **DRPG**'s policy, is not detrimental to **DRPG**'s best interests, and does not interfere with an team members regular work duties.

8.2 Team members are prohibited from revealing any **DRP** confidential or proprietary information or any other material covered by **DRPG**'s Information and Classification policy (DRPG 24 ISMS 8.2 DOC IS Classification Guidelines.docx) when engaged in blogging or social media.

8.3 Team members shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of drp and/or any of its team members. Team members are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging.

8.4 Team members may also not attribute personal statements, opinions or beliefs to drp when engaged in blogging or posting to social media. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of drp. Team members assume any and all risk associated with blogging.

8.5 Apart from following all laws pertaining to the handling and disclosure of copyrighted or export-controlled materials, **DRPG**'s trademarks, logos and any other **DRPG** intellectual property may also not be used in connection with any blogging activity unless express permission has come from the PR & Marketing dept.

8.6 Team members are not to publish, post or release any information that is considered confidential or not public. If there are questions about what is considered confidential, team members should check with their Line Manager or Information Security Manager.

8.7 Team members should get appropriate permission before you refer to, or post images of current or former team members, vendors or suppliers. Additionally, team members should get appropriate permission to use a third party's copyrights, copyrighted material, trademarks, service marks or other intellectual property.

8.8 When using **DRPG** computer systems, use of social media for business purposes is allowed but personal use of social media networks or personal blogging of online content is discouraged and could result in disciplinary action.

9 Security

9.1 Team members will not seek to avoid and will uphold **DRPG**'s anti-malware / anti-virus policies and procedures, will not intentionally interfere in the normal operation of the network or take any steps that substantially hinder others in their use of the network, and will not examine, change or use another person's files or any other information asset for which they don't have the owner's explicit permission.

10 Monitoring

10.1 All **DRPG** resources, including computers, email and voicemail are provided for business purposes and may be subject to monitoring for security and network management and users may have their usage of these resources subjected to limitations by **DRPG**. **DRPG** does not routinely monitor email, internet traffic or other uses of IT, however monitoring software is constantly recording network activity including that of individual workstations and this system may be used to undertake spot checks or investigations into employee activity if necessary.

11 Document owner and validity

The Information Security Manager is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the requirements of the ISMS.

This document is valid from 24/01/2022

Next review date 23/01/2023

12 Change Record

Issue	Description of change	Approved by	Date
1	Re-issue and renumbered. Updated policy template. Annual review.	Richard Parmenter	21/01/2022