

WEGENER INTERNET PROTOCOL

Rules Governing the Use of the Internet and Email at Koninklijke Wegener NV

Article 1

Scope

1. This Internet Protocol applies to all people – hereafter referred to as ‘users’ – working for Koninklijke Wegener NV and its Netherlands-based business units, hereafter referred to as ‘Wegener’.
2. Before granting users internet access, the employer will provide them with a copy of this Internet Protocol. The users are required to sign the enclosed statement as correct to indicate that they are familiar with the substance of this Internet Protocol.

Article 2

General principles

1. Internet access comprises the use of various services, notably email, intranet and the World Wide Web (WWW or web surfing). Whenever the term ‘the internet’ is used in this document, it refers to any of these services.
2. In the Wegener organisation, many users have to use the internet for the proper performance of their duties. Inappropriate use of this medium takes up time and capacity of people and equipment and may cause damage to ICT facilities, business processes or products. It can also result in the leaking of business secrets and damage to the reputation of the company and people.
3. Given these risks, Wegener expects professional and honest conduct from users.
4. To prevent such risks, Wegener issues various regulations governing the performance of work, the supervision of work, and the ability to take measures to facilitate effective business operations. The guidelines and rules described in this Internet Protocol form part of these regulations.
5. Internet use is automatically logged to safeguard the continuity of the technical infrastructure and to prevent interruption of business processes and other (financial) damage. These logs can be used to check and supervise compliance with the Internet Protocol.
6. The registration of personal data is governed by the Personal Data Protection Act (abbreviated to WBP in Dutch), as is the logging referred to in this Internet Protocol. The WBP defines personal data as ‘any information relating to an identified or identifiable individual’.
7. Data that can be reduced to an individual will only be provided for the purpose of supervision on a need-to-know basis. Wegener strives for a good balance between management of ICT resources and protection of users’ privacy. Internet use will only be checked if Wegener has reason to suspect infringement of the Internet Protocol or serious malfunction of ICT resources.

8. Anyone taking cognisance of logged information and the resulting research data is obligated to observe strict confidentiality in relation to the same.
9. Infringements may be grounds for disciplinary action and measures relating to employment law.

Article 3

Internet use

1. Users can access the internet via Wegener’s network with a user ID (logon name) and password, which are strictly personal and are not to be disclosed to any third parties. User IDs are associated with different authorisations that determine the functionality the user in question can access. Users are not permitted to access the internet in any other way.
2. All users are personally responsible for compliance with the guidelines and rules stipulated in this Internet Protocol, and are required to deal responsibly with information found on the internet.
3. As users are granted internet access for business purposes, its use should be related to the duties associated with their position.
4. Occasional, brief private internet use is permitted, provided that it does not disrupt the user’s work and the operation of ICT facilities, and that the rules defined in this Internet Protocol are respected.
5. Users are not permitted to use the internet:
 - > to conduct business with no bearing on Wegener;
 - > to send messages with pornographic, racist, discriminatory, abusive or otherwise offensive content;
 - > to visit websites containing such material;
 - > to gamble;
 - > to distribute or forward chain letters and visit chat rooms;
 - > to gain unauthorised access to computer systems (‘hacking’);
 - > to download music, film and other files for personal use;
 - > for any other indecent, irresponsible or illegitimate purposes.
6. Wegener reserves the right to take technical measures to block access to certain sites, filter mail content and block certain types of files.
7. The provisions of Article 3.5 do not apply if users must be able to perform such activities for the performance of their duties, provided that such activities do not contravene the law and are not harmful to the ICT facilities. For these activities, employees require their manager’s permission on a per assignment basis.
8. Installing and modifying hardware is the exclusive domain of the ICT administration department. The same applies to downloading, installing and modifying software and applications. Users are therefore not authorised to do so, unless they are given permission



by the ICT administration department. Such permission is required for each download, installation or modification.

9. Confidential company information may only be disclosed to third parties with the permission of the most senior manager and only if such disclosure is required in relation to the user's duties. Electronic transmission is only permitted if it is permissible to provide the information as hard copy. Electronic dissemination, especially using email, involves a significant risk of mistakes and therefore requires particular caution on the part of users.
10. Wegener reserves the right to add a disclaimer to outgoing emails. This disclaimer notifies all recipients, especially unintended recipients, of their obligation to handle any information received with caution.

Article 4

Registration and checks

1. Incoming and outgoing internet traffic is checked for viruses. The majority of viruses are automatically blocked and removed. If, nonetheless, a virus report appears on screen, the recipient should notify the service desk immediately and resume work only after the service desk has given permission.
2. Internet traffic data is reported on at the aggregate level and cannot readily be reduced to individual users.
3. Analysis and checks are normally limited to traffic data.
4. Targeted checks will be conducted if a user or group of users is strongly suspected of infringing rules.
5. Content will only be checked if there are weighty reasons to do so.
6. Email is considered personal mail. Its content will only be checked if it is strongly suspected of being in contravention of this Internet Protocol.
7. The checks referred to in Articles 4.4 to 4.6 inclusive are subject to the procedure appended to this Internet Protocol.
8. In other cases, emails may only be read by a person other than the user if the user has given permission for it.
9. Email exchanged between members of the works council and email from company medical officers and other people occupying a confidential position are normally excluded from checks, apart from checks concerning the security of email traffic.
10. Logs and reports are saved until the ICT administration department no longer needs them for the performance of its tasks. Inspection data that can be reduced to an individual is not kept any longer than necessary, in any event no longer than six months, barring the provisions of Article 15 of the Appendix.

Article 5

User rights

1. Users are entitled to take cognisance of the type of data logged with regard to internet use.
2. Users are entitled to access the information collected on them pertaining to an investigation of a suspected infringement.
3. If users feel disadvantaged under this Internet Protocol, they may invoke Koninklijke Wegener's Regulations Governing the Right of Complaint.

Article 6

Sanctions

1. In the event of and depending on the nature and severity of an infringement of this Internet Protocol, action may be taken, including disciplinary action and measures relating to employment law, such as revocation of the right to internet use, termination of the employment contract and reporting to the police.
2. Violating the confidentiality of registered information, the investigations or conclusions of investigations is regarded as a severe infringement and will be handled as such.

Article 7

Conclusion

1. The Board of Directors of Koninklijke Wegener NV will decide in the event of situations not provided for by this Internet Protocol.
2. This Internet Protocol has been approved by the central works council of Koninklijke Wegener NV.
3. This Internet Protocol came into effect on 12 May 2005.

This Internet Protocol applies to staff of or working for:

- > Koninklijke Wegener NV
- > Wegener Nederland BV
- > Wegener NieuwsMedia BV
 - Brabants Dagblad
 - Eindhovens Dagblad
 - De Twentsche Courant Tubantia
 - De Gelderlander
 - de Stentor
 - BN/DeStem | PZC
 - Uitgeverij BN/DeStem BV
 - Uitgeverij Provinciale Zeeuwse Courant BV
- > Wegener Huis-aan-huisMedia BV

- > Wegener NieuwsDruk BV (staf)
 - Wegener NieuwsDruk Best
 - Wegener NieuwsDruk Gelderland
 - Wegener NieuwsDruk Twente
 - Wegener NieuwsDruk Nijmegen
 - Wegener NieuwsDruk Brabant
 - Wegener NieuwsDruk West
- > Wegener ICT | Media BV
- > Wegener Facilitair Bedrijf BV
- > Wegener MediaVentions BV

Procedure for investigating suspected infringements of the Internet Protocol

1. In the interest of both the investigation and the user in question, as few officers as possible will be involved in the investigation. Each officer involved in the investigation is required to monitor this carefully.
2. An investigation into a suspected infringement of the Internet Protocol by individual users can only be initiated by the department's most senior manager after consulting the head of P&O, in the form of a written assignment.
3. The head of P&O assesses whether the most senior manager's assignment meets the following requirements:
 - > the request for the investigation is properly substantiated;
 - > the object of the investigation is clearly described;
 - > the investigation will not extend beyond what is strictly necessary;
 - > and then approves the investigation.
4. The head of P&O sends the request to the head of the ICT administration department.
5. The head of the ICT administration department assesses the request and starts the investigation if he/she agrees with the request.
6. The most senior manager informs the user involved as soon as possible of the pending investigation into his/her internet use, the reason for it and possibly its expected duration.
7. The head of the ICT administration department will ensure that the investigation progresses properly as long as it is underway, serve as the point of contact for the head of P&O and ensure that the investigation is conducted in a timely and appropriate manner.
8. At the start of the investigation, all potentially relevant data is secured to allow it to be used as evidence, and the most senior manager is notified upon completion of this step.
9. The people placed in charge of the investigation by the head of the ICT administration department are permitted to use all necessary information included in the objects to be checked by them. These employees are also bound to the obligation to observe strict confidentiality with regard to the investigation, the user or users involved and any conclusions. Email will therefore not be used to communicate about the investigation, and all information regarding the investigation will be saved securely at a location only accessible to those authorised to do so, both during and after the investigation. The investigators have to keep a log of the manner in which the investigation was carried out and the data used.
10. The content of email may only be investigated by the head of P&O and only in so far as this is strictly necessary.
11. The head of the ICT administration department reports the substantiated findings of the investigation in writing to the head of P&O. The head of P&O notifies the user involved and the most senior manager of the results and the preliminary conclusions of the investigation.
12. Users will be given the opportunity to respond to the accusation and granted access to the data collected on them as part of the investigation.
13. The most senior manager and the head of P&O will decide what steps to take next and notify the user of their decision.
14. If the investigation leads to the conclusion that no infringement has taken place, the ICT administration department will destroy all investigational data at once. The user involved will be informed in writing that he/she has not been found culpable in any way under this Internet Protocol or that any activities observed have not been found to be illegitimate.
15. If the investigation leads to the conclusion that the user is culpable of an infringement, the investigational data is offered to the head of P&O for further handling and filing. The most senior manager will notify his/her immediate manager of this. All documents will be kept by P&O for three years, after which they will be destroyed. The original written assignment and conclusion of the investigation, including the action taken, will be included in the user's personnel file.
16. If the outcome of the investigation leads to the conclusion that the user's employment contract should be terminated, the most senior manager and the head of P&O will propose this to the executive and the executive will take a final decision in this matter.



