

**positive
planet**

**Information Management &
Data Security Policy**

Version 1.03
April 2024

Policy statement

Positive Planet recognises that it has a responsibility to safeguard information belonging to Positive Planet and its stakeholders (third parties and customers) within a secure environment. It requires all users to exercise a duty of care in relation to the operation and use of its information systems. Positive Planet will comply with all relevant legislation applicable to the use of IT and all related digital facilities.

Responsibility

The Directors are responsible for ensuring that the Security and Protection of Information Policy is implemented. However, all employees have a responsibility in their area to ensure that the aims and objectives of the policy are met.

Tom Constantine is the Data Protection Officer.

Policy aims

- Protect company, customer and employee data
- Keep valuable company information secret
- Meet our legal obligations under the General Data Protection Regulation and other laws
- Meet our professional obligations towards our customers and third parties.

Practical arrangements

Customer information and systems:

Positive Planet signs mutual NDA agreements with its customers and sub-contractors and operates in compliance with the GDPR 'Right to Access'. This is the right of data subjects to obtain confirmation as to whether we are processing their data, where we are processing it and for what purpose.

All Positive Planet staff working with customer information are bound under non-disclosure conditions specified in their contract of employment.

Access to the customer's production environment and other test environments containing production data held on the customer's site is granted via a user account provided to Positive Planet by the customer and which holds elevated permissions so as to allow access to the elements of the solution for investigation. Positive Planet support staff and sub-contractors can access all of the customers' production data, unless specific arrangements have been made to the contrary. Positive Planet support staff will only access customer information in connection with the issue they are investigating.

Positive Planet has a duty of information security when sharing usernames & passwords, no matter whether or not the customer is happy to send username & password in the same document.

- Either send the username and password using separate mechanisms e.g. password by text message and username by email; or
- Encrypt the information in a document and send the password to that document again by a separate mechanism.
- Customer passwords should be stored in a password management system.

Internal information and systems

As far as possible, Positive Planet operates on a 'need to share' rather than a 'need to know' basis with respect to company confidential information. This means that our bias and intention is to share information to help people do their jobs rather than raise barriers to access needlessly.

Effective security is a team effort requiring the participation and support of every employee and associate. Employees are responsible for knowing and following these guidelines and are personally responsible for the secure handling of confidential information that is entrusted to them. Employees may access, use or share confidential information only to the extent it is authorised and necessary for the proper performance of your duties. Promptly report any theft, loss or unauthorised disclosure of protected information or any breach of this policy to a company Director.

All employees must participate in the Cyber Security training program provided by Positive Planet. All employees must comply with the requirements of all relevant legislation. An employee must not interfere with the work of others or the system itself. The facilities must be used in a legal and responsible manner. Employees 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 for playing games
- Use for any kind of personal gain (e.g. advertising goods or services)
- Engage in activities which waste resources 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 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
- Send electronic mail, which is irresponsible, or likely to cause offence.

Social media

Social Media is used by Positive Planet as an integral part of its modern and interactive marketing and promotional activities. As ambassadors for Positive Planet, every employee is encouraged to actively support the Company's social media profile. An employee or ex-employee must not use any social media platform or similar to publish or distribute material that may undermine public confidence in Positive Planet, or in any way damage or harm the Company's reputation and standing. Any apparent breach by an employee of the Company's IT security and social media regulations will be referred to the Disciplinary Procedure.

Access

An employee must not gain unauthorised access to, or violate, the privacy of other peoples' files, corrupt or destroy other peoples' data or disrupt the work of other people. It is each employee's responsibility to prevent inappropriate access to their work files. Passwords must be kept safe, changed regularly and not be disclosed to anyone.

AI Powered Chatbots

As we embrace the transformative potential of AI-powered chatbots, such as ChatGPT and Google Bard, in our workplace, it is crucial for employees to exercise responsible and ethical use. Users are expected to refrain from sharing any confidential information related to the organization, including details about clients, employees, financial information, security measures, and other proprietary data when interacting with AI-powered chatbots.

AI usage must strictly adhere to all applicable laws and regulations. This encompasses compliance with data protection policies, intellectual property laws, and any specific regulations pertinent to the industry or sector

in which Positive Planet operates. Personal data handling must align with the organization's data protection policies.

Although AI-powered chatbots have come a long way, it is important that you are aware that their responses may not always be accurate, reliable, or free from bias. Human judgment must play a role in critical decision-making processes, and we expect you to validate any generated content, addressing any bias, and ensure its accuracy before integrating it into your work.

Guidance on interacting with AI-powered chatbots securely is integrated into the Cyber Security training program, emphasizing responsible AI use.

Privacy Policy

Positive Planet operates in compliance with requirements of the General Data Protection Regulation (GDPR). Our Privacy Policy is contained in the document Positive Planet HR - GDPR Commercial Activities Privacy Notice.PDF accessible via Positive Planet HR Database or on the Positive Planet website (<https://www.positiveplanet.co.uk/privacy-policy/>).

For and on behalf of Positive Planet Limited

Approved by: Stephen Henry | CEO @ Positive Planet



Date: 3 April 2024