

Privacy Policy (Surfprotect Chrome Extension)

The Privacy Policy statement applies to information which is collected from use of the Surfprotect Chrome Extension, it does not apply to any sites linked to as a result of using the extension.

We have a legal duty to protect any personal information we collect and take appropriate measures to do so.

Exa Networks' Policy Information

All documents on the Document Management System are live and present. Documents received in PDF format are uncontrolled and at the time of download.

Version Control

Title	Version	Reviewed By	Approved	Confidentiality
Privacy Policy (Surfprotect Chrome Extension)	1.0	Liane Farrell 20/08/2021	Thomas Mangin 20/08/2021	Public

Change History

▼ [Click here to expand...](#)

Version	Date	Author	Description of Change
1.0	20/08/2021	Liane Farrell	Conversion from draft to publication

Scope and Responsibilities

Scope

Exa Networks' policies and procedures apply to all staff and third parties, including, but not limited to; contractors, agency workers, permanent employees, associates and students operating on behalf of Exa Networks or accessing the company services at;

Exa Networks Limited 100 Bolton Road Bradford BD1 4DE

Responsibilities

- The Directors of Exa Networks retain overarching responsibility for the confidentiality, integrity and availability of corporate data
- The Directors ensure the continued suitability, effectiveness and relativity of all Exa Networks' policies and procedures, through periodic review. The compilation, amendment and distribution of associated documentation requires Director approval
- Department Managers are responsible for ensuring that staff remain compliant with Exa Networks' policies and procedures, through completing appropriate, formal and informal, assessments. Department Managers are to ensure that all staff have received adequate training in order to meet the outlined requirements, including both new-starters and existing employees
- Should any instances of non-conformance occur, Department Managers are responsible for ensuring that the Information Governance Department are notified. Department Managers are responsible for the facilitation of internal and external audits within their domain, allowing for necessary accommodations to be made and ensuring that any identified corrective action is applied/adopted
- Individual staff members are responsible for ensuring that all activity and individual work remains in accordance with the requirements of internal policies and procedures. Inclusive of those retained on the document management system and within the staff handbook and health and safety handbook. Should further information be required to assist with the understanding of company policy and procedures, the staff member is required to notify their line manager (in the first instance). Alternatively, the staff member shall contact the Information Governance department
- The Information Governance Department is responsible for the maintenance, generation and communication of Exa Networks' policies and procedures, including the; compilation, update and distribution of all associated documentation (as required), as well as the facilitation of staff training and verification of organisational compliance, through the completion of scheduled internal audits.

Non-conformance

All policies require the full participation of staff and contractors to be successful. Failure to comply with the requirements outlined within Exa Networks' policies and procedures constitutes misconduct and may result in disciplinary action, up to and including dismissal.

Privacy Policy (Surfprotect Chrome Extension)

Purpose, Scope and Users

The Privacy Policy statement applies to information which is collected from use of the Surfprotect Chrome Extension, it does not apply to any sites linked to as a result of using the extension.

We have a legal duty to protect any personal information we collect and take appropriate measures to do so.

All information is handled lawfully in accordance with the Data Protection Act 2018 (as amended from time to time).

Surfprotect is a content filtering solution for businesses and schools allowing the fulfilment of safeguarding requirements.

Surfprotect Extension facilitates the use of the SurfProtect products through a chrome browser.

Your Personal Information

Any personal information is held safely with our security systems preventing unauthorised access. This information will be treated in confidence and only used for the purposes for which it was provided. Exa Networks will not sell or rent your personally identifiable information to anyone. If we change our Privacy Policy, we will post any changes on this website so that you are always aware of how we use your information.

Exa Networks are committed to protecting the privacy of our users, clients and customers. This privacy statement explains how we use any personal information we collect about you when you use SurfProtect Extension. It is also intended to assist you in making informed decisions when using our Surfprotect Extension and our products and services.

All your personal Information shall be held and used in accordance with the General Data Protection Regulation. If you want to know what information we collect and hold about you, please email us at DPO@exa.net.uk or by writing to the Data Protection Officer, Exa Networks, 100 Bolton Road, Bradford, BD1 4DE

What Information Do We Collect?

The information we collect includes the personal information you provide to us when installing and logging into the SurfProtect Extension, such as your name and a password. We also process the content you upload or receive from others in order to deliver the features of SurfProtect when using our services. This is done in the form of web browsing logs when filtering the internet using Surfprotect. Web browsing logs are for the use of the user and the administrator(s) of Exa Networks' SurfProtect web filtering products.

The information we store includes scheme, host, path, query and time.

The information may be linked to an active directory profile and displayed as analytical data including IP address(es), username and group name.

How Do We Use Your Information?

The information which you provide to Exa Networks will be used within the company for the administration of any of Exa Networks' related products and services of which you avail. Data may also be used for statistical analyses and Exa Networks may share information with law enforcement bodies/ fraud prevention agencies for the purpose of preventing or detecting fraud. We may share your data with trusted third parties who process data on our behalf in line with this privacy policy.

Your Rights

Under GDPR, individuals now have increased rights in regard to their personal data. Please see below an outline of your rights and if you wish to contact us to discuss or amend the data we hold, please contact us DPO@exa.net.uk

- Right to be Informed
- Right of Access
- Right to Rectification
- Right to Erasure
- Right to Restrict Processing
- Right to Data Portability
- Right to Object
- The Right not to be Subject to Automated Decision-Making Including Profiling

Data Breach

If Exa Networks were to experience a data breach they would:

- Within 72 hours upon realising a breach had occurred and where feasible, report certain types of personal data breach to the relevant supervisory authorities.
- If the breach is likely to result in a high risk of adversely affecting our customer's individual rights and freedoms, we will also inform those individuals without undue delay.

Validity and Document Management

The owner of this document is the Information Governance Team (information.governance@exa.net.uk) who must check and, if necessary, update the document at least once a year.