

Privacy Policy & Cookies Statement

Privacy Policy

1. Introduction

This Policy sets out the obligations of Gem Cable Solutions Ltd ("the Company") regarding data protection and the rights of employees, customers, suppliers, complainants and enquirers ("data subjects") in respect of their personal data under EU Regulation 2016/679 General Data Protection Regulation ("GDPR"). The GDPR defines "personal data" as any information relating to an identified or identifiable natural person (a "data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

This Policy sets the Company's obligations regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out herein must be followed at all times by the Company, its employees, agents, contractors, or other parties working on behalf of the Company. The Company is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

2. The Data Protection Principles

This Policy aims to ensure compliance with the GDPR. The GDPR sets out the following principles with which any party handling personal data must comply. All personal data must be:

2.1 Processed lawfully, fairly, and in a transparent manner in relation to the data subject.

2.2 Collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

2.3 Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.

2.4 Accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay.

2.5 Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, subject to implementation of the appropriate technical

Setting the Standard for UK Cabling Solutions

Unit C, 156 St Albans Road, Sandridge, St. Albans, Herts, AL4 9LP, United Kingdom

+44 (0)1727 845750 info@gemcable.co.uk www.gemcable.co.uk

GEM Cable Solutions Registered in England. Company No. 5151023. VAT No. 842 7426 21



and organisational measures required by the GDPR in order to safeguard the rights and freedoms of the data subject.

2.6 Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

3. The Rights of Data Subjects

The GDPR sets out the following rights applicable to data subjects (please refer to the parts of this policy indicated for further details):

- 3.1 The right to be informed (Part 12).
- 3.2 The right of access (Part 13);
- 3.3 The right to rectification (Part 14);
- 3.4 The right to erasure (also known as the 'right to be forgotten') (Part 15);
- 3.5 The right to restrict processing (Part 16);
- 3.6 The right to object (Part 17); and

4. Lawful, Fair, and Transparent Data Processing

4.1 The GDPR seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The GDPR states that processing of personal data shall be lawful if at least one of the following applies:

- 4.1.1 The data subject has given consent to the processing of their personal data for one or more specific purposes;
- 4.1.2 The processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract with them;
- 4.1.3 The processing is necessary for compliance with a legal obligation to which the data controller is subject;
- 4.1.4 The processing is necessary to protect the vital interests of the data subject or of another natural person;
- 4.1.5 The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller; or
- 4.1.6 The processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Data Protection Policy (GDPR) v2.1 3

5. Specified, Explicit, and Legitimate Purposes

5.1 The Company collects and processes the personal data set out in Part 18 of this Policy. This includes:

5.1.1 Personal data collected directly from data subjects, for example, contact details used when a data subject communicates with us.

5.1.2 Personal data obtained from third parties, for example, contact details used from a 3rd party data provider for marketing purposes or sales leads provided by our product partners.

5.2 The Company only collects, processes, and holds personal data for the specific purposes set out in Part 18 of this Policy (or for other purposes expressly permitted by the GDPR).

5.3 Data subjects are kept informed at all times of the purpose or purposes for which the Company uses their personal data. Please refer to Part 12 for more information on keeping data subjects informed.

6. Adequate, Relevant, and Limited Data Processing

The Company will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed) as under Part 5, above, and as set out in Part 18, below.

7. Accuracy of Data and Keeping Data Up-to-Date

7.1 The Company shall ensure that all personal data collected, processed, and held by it is kept accurate and up-to-date. This includes, but is not limited to, the rectification of personal data at the request of a data subject, as set out in Part 14, below.

7.2 The accuracy of personal data shall be checked when it is collected and at regular intervals thereafter. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

8. Data Retention

8.1 The Company shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed.

8.2 When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.

9. Secure Processing

The Company shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage. Further details of the technical and organisational measures which shall be taken are provided in Parts 19 to 24 of this Policy. Data Protection Policy (GDPR) v2.1 4

10. Accountability and Record-Keeping

10.1 The Company's Data Protection Officer is Jon Mallard, who can be contacted at Open Reality Ltd, 10 Hitching Court, Abingdon Business Park, Abingdon, Oxfordshire, OX14 1RG.

10.2 The Data Protection Officer shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, the Company's other data protection-related policies, and with the GDPR and other applicable data protection legislation.

10.3 The Company shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

10.3.1 The name and details of the Company, its Data Protection Officer, and any applicable third-party data processors;

10.3.2 The purposes for which the Company collects, holds, and processes personal data;

10.3.3 Details of the categories of personal data collected, held and processed by the Company, and the categories of data subject to which that personal data relates;

10.3.4 Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards;

10.3.5 Details of how long personal data will be retained by the Company (please refer to the Company's Data Retention Policy); and

10.3.6 Detailed descriptions of all technical and organisational measures taken by the Company to ensure the security of personal data.

11. Data Protection Impact Assessments

11.1 The Company shall carry out Data Protection Impact Assessments for any and all new projects and/or new uses of personal data.

11.2 Data Protection Impact Assessments shall be overseen by the Data Protection Officer and shall address the following:

11.2.1 The type(s) of personal data that will be collected, held, and processed;

11.2.2 The purpose(s) for which personal data is to be used;

11.2.3 The Company's objectives;

11.2.4 How personal data is to be used;

11.2.5 The parties (internal and/or external) who are to be consulted;

11.2.6 The necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;

11.2.7 Risks posed to data subjects;

11.2.8 Risks posed both within and to the Company; and

11.2.9 Proposed measures to minimise and handle identified risks.
Data Protection Policy (GDPR) v2.1 5

12. Keeping Data Subjects Informed

12.1 The Company shall provide the information set out in Part 12.2 to every data subject:

12.1.1 Where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and

12.1.2 Where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose:

a) if the personal data is used to communicate with the data subject when the first communication is made; or
b) if the personal data is to be transferred to another party before that transfer is made; or

12.2 The following information shall be provided:

12.2.1 Details of the Company including, but not limited to, the identity of its Data Protection Officer;

12.2.2 The purpose(s) for which the personal data is being collected and will be processed (as detailed in Part 18 of this Policy) and the legal basis justifying that collection and processing;

12.2.3 Where applicable, the legitimate interests upon which the Company is justifying its collection and processing of the personal data;

12.2.4 Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;

12.2.5 Where the personal data is to be transferred to one or more third parties, details of those parties;

12.2.6 Where the personal data is to be transferred to a third party that is located outside of the European Economic Area (the "EEA"), details of that transfer, including but not limited to the safeguards in place (see Part 25 of this Policy for further details);

12.2.7 Details of data retention;

12.2.8 Details of the data subject's rights under the GDPR;

12.2.9 Details of the data subject's right to withdraw their consent to the Company's processing of their personal data at any time;

12.2.10 Details of the data subject's right to complain to the Information Commissioner's Office (the "supervisory authority" under the GDPR);

12.2.11 Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it; and

12.2.12 Details of any automated decision-making or profiling that will take place using the personal data, including information on how decisions will be made, the significance of those decisions, and any consequences.

Data Protection Policy (GDPR) v2.1 6

13. Data Subject Access

13.1 Data subjects may make subject access requests ("SARs") at any time to find out more about the personal data which the Company holds about them, what it is doing with that personal data, and why.

13.2 Data subjects wishing to make a SAR may do so in writing to the Company's Data Protection Officer at Open Reality Ltd, 10 Hitching Court, Abingdon Business Park, Abingdon, OX14 1RG.

13.3 Responses to SARs shall normally be made within one month of receipt, however, this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.

13.4 All SARs received shall be handled by the Company's Data Protection Officer.

13.5 The Company does not charge a fee for the handling of normal SARs. The Company reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

14. Rectification of Personal Data

14.1 Data subjects have the right to require the Company to rectify any of their personal data that is inaccurate or incomplete.

14.2 The Company shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing the Company of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

14.3 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

15. Erasure of Personal Data

15.1 Data subjects have the right to request that the Company erases the personal data it holds about them in the following circumstances:

15.1.1 It is no longer necessary for the Company to hold that personal data with respect to the purpose(s) for which it was originally collected or processed;

15.1.2 The data subject wishes to withdraw their consent to the Company holding and processing their personal data;

15.1.3 The data subject objects to the Company holding and processing their personal data (and there is no overriding legitimate interest to allow the Company to continue doing so) (see Part 17 of this Policy for further details concerning the right to object);

15.1.4 The personal data has been processed unlawfully;

15.1.5 The personal data needs to be erased in order for the Company to comply with a particular legal obligation.

Data Protection Policy (GDPR) v2.1 7

15.2 Unless the Company has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

15.3 In the event that any personal data that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

16. Restriction of Personal Data Processing

16.1 Data subjects may request that the Company ceases processing the personal data it holds about them. If a data subject makes such a request, the Company shall retain only the amount of personal data concerning that data subject (if any) that is necessary to ensure that the personal data in question is not processed further.

16.2 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

17. Objections to Personal Data Processing

17.1 Data subjects have the right to object to the Company processing their personal data based on legitimate interests, direct marketing (including profiling).

17.2 Where a data subject objects to the Company processing their personal data based on its legitimate interests, the Company shall cease such processing immediately, unless it can be demonstrated that the Company's legitimate grounds for such processing override the data subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.

17.3 Where a data subject objects to the Company processing their personal data for direct marketing purposes, the Company shall cease such processing immediately.

18. Personal Data Collected, Held, and Processed

The following personal data is collected, held, and processed by the Company:

18.1 Names of Individuals – Will include contact names of customers, suppliers, staff and those in our marketing database (including job titles). The names are stored and used to facilitate contact with those individuals. Names of staff are held in HR files together with other personal data required to process payroll.

18.2 Postal addresses – Personal addresses for staff are held in the HR files to facilitate contact for payroll and pension purposes. No personal addresses are held in respect of other contacts.

18.3 Email addresses – Collected and held in the course of communicating with contacts and those in our marketing database.

18.4 Telephone numbers – Collected and held in the course of communicating with
Data Protection Policy (GDPR) v2.1 8
contacts and those in our marketing database.

19. Data Security - Transferring Personal Data and Communications

The Company shall ensure that the following measures are taken with respect to all communications and other transfers involving personal data:

19.1 All emails containing personal data must be encrypted.

19.2 All emails containing personal data must be marked “restricted”;

19.3 Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted under any circumstances;

19.4 Where personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data;

19.5 Where personal data is to be transferred in hardcopy form it should be passed directly to the recipient or sent via recorded delivery.

20. Data Security - Storage

The Company shall ensure that the following measures are taken with respect to the storage of personal data:

20.1 All electronic copies of personal data should be stored securely using passwords and data encryption;

20.2 All hard copies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar;

20.3 All personal data stored electronically should be backed up. All backups should be encrypted;

20.4 No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets, and smartphones), whether such device belongs to the Company or otherwise without the formal written approval of the director responsible for the safekeeping of that information and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary; and

20.5 No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Company where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the GDPR (which may include demonstrating to the Company that all suitable technical and organisational measures have been taken).

21. Data Security - Disposal

When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. For further information on the deletion and disposal of personal data, please refer to the Company's Data Retention Policy. Data Protection Policy (GDPR) v2.1 9

22. Data Security - Use of Personal Data

The Company shall ensure that the following measures are taken with respect to the use of personal data:

22.1 No personal data may be shared informally and if an employee, agent, sub-contractor, or other party working on behalf of the Company requires access to any personal data that they do not already have access to, such access should be formally requested from the director responsible for the safekeeping of that information;

22.2 No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Company or not, without the authorisation of the director responsible for the safekeeping of that information;

22.3 Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors, or other parties at any time;

22.4 If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it; and

22.5 Where personal data held by the Company is used for marketing purposes, it shall be the responsibility of the Marketing Manager to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service such as the TPS.

23. Data Security - IT Security

The Company shall ensure that the following measures are taken with respect to IT and information security:

23.1 Passwords are used to protect personal data, in line with our Information Security Management System.

23.2 Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of the Company, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method.

23.3 All software (including, but not limited to, applications and operating systems) shall be kept up-to-date. The Company's IT staff shall be responsible for installing any and all security-related updates as soon as reasonably and practically possible unless there are valid technical reasons not to do so.

24. Organisational Measures

The Company shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

24.1 All employees, agents, contractors, or other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company's responsibilities under the GDPR and under this Policy and shall be provided with a copy of this Policy;

24.2 Only employees, agents, sub-contractors, or other parties working on behalf of
Data Protection Policy (GDPR) v2.1 10

the Company that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Company;

24.3 All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately trained to do so;

24.4 All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately supervised;

24.5 All employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise;

24.6 Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;

24.7 All personal data held by the Company shall be reviewed periodically, as set out in the Company's Data Retention Policy;

24.8 The performance of those employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed;

24.9 All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be bound to do so in accordance with the principles of the GDPR and this Policy by contract;

24.10 All agents, contractors, or other parties working on behalf of the Company handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Company arising out of this Policy and the GDPR; and

24.11 Where any agent, contractor or other party working on behalf of the Company handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

25. Transferring Personal Data to a Country Outside the EEA

25.1 The Company may from time to time transfer ('transfer' includes making available remotely) personal data to countries outside of the EEA.

25.2 The transfer of personal data to a country outside of the EEA shall take place only if one or more of the following applies:

25.2.1 The transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the European Commission has determined ensures an adequate level of protection for personal data;

25.2.2 The transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the European Commission; compliance with an approved

code of conduct approved by a supervisory authority (e.g. the Information Commissioner's Office); certification under an approved certification mechanism (as provided for in the GDPR); contractual clauses agreed and authorised by the Data Protection Policy (GDPR) v2.1 11 competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority;

25.2.3 The transfer is made with the informed consent of the relevant data subject(s);

25.2.4 The transfer is necessary for the performance of a contract between the data subject and the Company (or for pre-contractual steps taken at the request of the data subject);

25.2.5 The transfer is necessary for important public interest reasons;

25.2.6 The transfer is necessary for the conduct of legal claims;

25.2.7 The transfer is necessary to protect the vital interests of the data subject or other individuals where the data subject is physically or legally unable to give their consent; or

25.2.8 The transfer is made from a register that, under UK or EU law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.

26. Data Breach Notification

26.1 All personal data breaches must be reported immediately to the Company's Data Protection Officer.

26.2 If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Officer must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

26.3 In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Part 26.2) to the rights and freedoms of data subjects, the Data Protection Officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.

26.4 Data breach notifications shall include the following information:

26.4.1 The categories and approximate number of data subjects concerned;

26.4.2 The categories and approximate number of personal data records concerned;

26.4.3 The name and contact details of the Company's data protection officer (or other contact point where more information can be obtained);

26.4.4 The likely consequences of the breach;

26.4.5 Details of the measures taken or proposed to be taken, by the Company to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

Data Protection Policy (GDPR) v2.1 12

Cookies Statement

Cookies are text files containing small amounts of information which are downloaded to your hard disk or to your browser's memory when you visit one of Gem Cable Solutions Ltd sites. Cookies are useful because they help arrange the content and layout of our sites and allow us to recognize those computers or other devices that have been to our sites before. Cookies do many different jobs, such as allowing our websites to remember your preference settings and helping us to enhance the usability and performance of our sites and your experience using them.

Our sites also may contain electronic images known as web beacons – sometimes called single-pixel gifs – that allow us to count the number of users who have visited specific pages. We may include web beacons in promotional e-mail messages or newsletters in order to determine whether messages have been opened and acted upon.

Cookie categories

The type of cookie that may be used on Gem Cable Solutions Ltd sites can be put into 1 of 4 categories: Strictly Necessary, Performance, Functionality & Profile and Advertising.

1. Strictly Necessary Cookies

These cookies are essential, as they enable you to move around our sites and use their features, particularly in connection with information searches and order placement. Without these cookies, services you have asked for cannot be provided. These cookies do not gather information about you that could be used for marketing or remembering where you have been on the internet. An example of a strictly necessary cookie is a “shopping basket cookie,” which is used to remember the products that you wish to purchase when you add products to your shopping basket or proceed to checkout.

2. Performance Cookies

These cookies collect information about how you use our sites, for example, which pages you go to most often and if you get any error messages from certain pages. These cookies collect only anonymous information that is used to improve how our sites work.

These cookies are not used to target you with online advertising. Without these cookies, we cannot learn how our sites are performing and make relevant improvements that could better your browsing experience. Examples of performance cookies that our sites use include Google and Adobe Analytics (see further discussion below).

3. Functionality & Profile Cookies

These cookies allow our sites to store information that you provide such as your site language preferences and to store technical information useful for your interactions with our sites. For instance, they remember

Setting the Standard for UK Cabling Solutions

Unit C, 156 St Albans Road, Sandridge, St. Albans, Herts, AL4 9LP, United Kingdom

+44 (0)1727 845750 info@gemcable.co.uk www.gemcable.co.uk

GEM Cable Solutions Registered in England. Company No. 5151023. VAT No. 842 7426 21



your user ID and elements of your user profile. They also ensure that your experience using the sites and Gem Cable Solutions Ltd marketing efforts are relevant to you. They may also be used to provide services you have asked for such as watching a video or commenting on a blog. The information these cookies collect may be anonymous and they cannot track your browsing activity on other websites.

Without these cookies, a website cannot remember choices you have previously made or personalize your browsing experience. For example, we use a cookie to store your language preferences, which allows us to present you with product search results in the correct language, and we use a cookie to store your choice about the appearance of the cookie information banner that we display on our sites. This cookie will help us remember your choice about the appearance of the cookie information banner when you subsequently visit the same site where you made your choice about the banner and any other Gem Cable Solutions Ltd sites with the same domain or the same top level domain.

4. Advertising Cookies

These cookies may be used to deliver advertisements that are more relevant to you and your interests. They may also be used to limit the times you see an advertisement as well as help to measure the effectiveness of the advertising campaign. Although these cookies may track your visits to other websites, they do not usually know who you are.

Without these cookies, online advertisements you encounter will be less relevant to you and your interests.

Setting your cookie preference

You have the ability to accept or decline cookies. Most internet browsers automatically accept cookies, but you can usually modify your browser settings to decline cookies or to notify you when a cookie is being placed on your computer. If you choose to decline cookies, you may not be able to fully experience the features of Gem Cable Solutions Ltd sites or other websites that you visit.

Our use of web analytics

Gem Cable Solutions Ltd uses industry standard web analytics to track visits to our sites. These analytics are provided by Google Analytics. The information generated by the cookie about your use of our sites (including your IP address) will be transmitted to and stored by Google on servers in the United States. Google will use this information for the purpose of evaluating your use of our sites, compiling reports on website activity for website operators and providing other services relating to website activity and internet usage. Google may also transfer this information to third parties where required to do so by law, or where such third parties process the information on Google's behalf. Google will not associate your IP address with any other data held by Google.

You may opt out of web analytics by installing these tools on your computer.

[Google Analytics Opt-Out Link](#)

Setting the Standard for UK Cabling Solutions

Unit C, 156 St Albans Road, Sandridge, St. Albans, Herts, AL4 9LP, United Kingdom

+44 (0)1727 845750 info@gemcable.co.uk www.gemcable.co.uk

GEM Cable Solutions Registered in England. Company No. 5151023. VAT No. 842 7426 21



Do-Not-Track Signals and Similar Mechanisms

Some web browsers may transmit “do-not-track” signals to the sites with which the user communicates. Because of differences in how web browsers incorporate and activate this feature, it is not always clear whether users intend for these signals to be transmitted, or whether they even are aware of them. There currently is disagreement, including among participants in the leading Internet standards-setting organization, concerning what, if anything, websites should do when they receive such signals.

Gem Cable Solutions Ltd currently does not take action in response to these signals. If and when a final standard is established and accepted, Gem Cable Solutions Ltd will reassess how to respond to these signals.

Implementation of Policy

This Policy shall be deemed effective as of 25th May 2018. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

Enforcement of this privacy statement/Contact Us

If you have questions regarding this statement or our handling of your personal information, please contact us using the contact information listed below. We will promptly address your concern and strive to reach a satisfactory resolution.

Email:

Gem Cable Solutions Ltd
privacy@gemcable.co.uk

Mailing Address:

Gem Cable Solutions Ltd Privacy
Unit C, 156 St Albans Road
Sandridge
St Albans
Hertfordshire
AL4 9LP

Changes to this privacy statement and Cookies Statement

Gem Cable Solutions Ltd may occasionally update this privacy statement. When we do, we will revise the “last updated” date at the top and bottom of the privacy statement. If we make any material changes in the way we collect, use and/or share personal information that we collect about you through the sites, we will notify you by sending you an email at the last email address that you provided us and/or by prominently posting notice of the changes on the sites.

Issue 1.1

Setting the Standard for UK Cabling Solutions

Unit C, 156 St Albans Road, Sandridge, St. Albans, Herts, AL4 9LP, United Kingdom

+44 (0)1727 845750 info@gemcable.co.uk www.gemcable.co.uk

GEM Cable Solutions Registered in England. Company No. 5151023. VAT No. 842 7426 21

