

GSS – Confidentiality and Privacy Policy

GSS is committed to protecting your privacy when you use our services.

This Confidentiality and Privacy policy explains how we use information about you and how we protect your privacy.

From 25 May 2018, your personal information will be processed, held and/or controlled in accordance with the General Data Protection Regulations (2016/679).

We have a Data Protection Officer who makes sure we respect your rights and follow the law. You may contact us at any time to:

- Request access to information which we have about you
- Correct any information which we have about you
- Ask for any information which we have about you to be deleted
- Discuss any concerns or ask any questions about how we look after your personal information

Please contact the Data Protection Officer – Richard Wood on richard@gss-ukltd.co.uk or by writing to:

Richard Wood, GSS UK Ltd
Square Root Business Centre
102-116 Windmill Road
Croydon, Surrey, CR0 2XQ

Information we collect

We may collect personal information about you including audio and video recordings. This can be anything that identifies and relates to a living person and can include information that when put together with other information can then identify the person. For example, this could be your name, contact details, email address and/or telephone number.

Did you know that some of your personal information might be ‘special’?

Some information is ‘special’ and needs more protection due to its sensitivity. It’s often information you would not want widely known and is very personal to you. This is likely to include anything that can reveal your:

- sexuality and sexual health
- religious or philosophical beliefs
- ethnicity
- physical or mental health
- trade union membership
- political opinion
- genetic/biometric data
- criminal history

Why do we need your personal information?

We may need to use some information about you to:

- deliver services and support to you
- manage those services we provide to you
- train and manage the employment of our workers who deliver those services
- help investigate any worries or complaints you have about your services and to answer your questions and enquiries
- allow you to participate in online training and interactive features of our services if you choose to
- check and improve the quality of our services
- help with research and planning of new services
- send you information which we think might be of interest to you if you have agreed to this
- third parties where we have retained them to provide services that we, you or our client have requested
- monitor compliance with our equal opportunities policy
- carry out our obligations arising from any contracts entered into between you and us
- market our related products and services to you, where you have given your consent for us to do so

We reserve the right to transfer your data if GSS is sold, goes into a merger, liquidation or receivership or transfers all, or substantially all, of its assets to a new owner. This will only take place if the third party agrees to adhere to the terms of this privacy statement. We will let you know of any such transfer and you will be able to opt-out if you wish.

How the law allows us to use your personal information

GSS processes personal data, both as a Data Controller and as a Data Processor, as defined by relevant Data Protection Legislation: the General Data Protection Regulations 2016/679, the Data Protection Act 1998, the EU Data Protection Directive 95/46/EC, the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699), the Electronic Communications Data Protection Directive 2002/58/EC, the Privacy and Electronic Communications (EC Directive) Regulations 2003 and all applicable laws and regulations relating to processing of personal data and privacy, including where applicable the guidance and codes of practice issued by the Information Commissioner.

There are a number of legal reasons why we need to collect and use your personal information. Generally, we collect and use personal information where:

- you, or your legal representative, have given consent
- you have entered into a contract with us
- it is necessary to perform our statutory duties
- it is required by law
- it is necessary for employment purposes
- you have made your information publicly available
- it is necessary for legal cases
- it is to the benefit of society as a whole
- it is necessary for archiving, research, or statistical purposes

If we have consent to use your personal information, rather than legal or contractual reasons, you have the right to remove it at any time. If you want to remove your consent, please contact GSS and tell us which service you're using so we can deal with your request.

We only use what we need

We'll only collect and use personal information if we need it to deliver a service or meet a requirement.

If we don't need personal information we'll either keep you anonymous if we already have it for something else or we won't ask you for it. For example, in a survey we may not need your contact details we'll only collect your survey responses.

If we use your personal information for research and analysis, we'll always keep you anonymous or use a different name unless you've agreed that your personal information can be used for that research.

We don't sell your personal information to anyone else.

What you can do with your information

The law gives you a number of rights to control what personal information is used by us and how it is used by us.

You can ask for access to the information we hold on you.

We would normally expect to share what we record about you with you, whenever we assess your needs or provide you with services.

However, you also have the right to ask for all the information we have about you and the services you receive from us. When we receive a request from you, we must give you access to everything we've recorded about you.

However, we can't let you see any parts of your record which contain:

- Confidential information about other people; or
- Data a professional advisor thinks will cause serious harm to your or someone else's physical or mental wellbeing; or
- If we think that giving you the information may stop us from preventing or detecting a crime

This applies to personal information that is in both paper and electronic records.

If you ask us for access to your information then we'll ask you to provide evidence so that we can verify your identity.

If you have any queries about access to your information please contact us.

You can ask to change information you think is inaccurate

You should let us know if you disagree with something written on your file.

We may not always be able to change or remove that information but we'll correct factual inaccuracies and may include your comments in the record to show that you disagree with it.

If you ask us to change the information we hold about you then we'll ask you to provide evidence so that we can verify your identity.

The quickest way to inform us of any inaccuracies is to complete a form which we can provide to you or you can talk to a member of staff, contact Sherella Mitchell, GSS Office Manager or write to us at:

Square Root Business Centre
102-116 Windmill Road
Croydon, Surrey, CR0 2XQ

You can ask to delete information (the right to be forgotten)

In some circumstances you can ask for your personal information to be deleted, for example:

- Where your personal information is no longer needed for the reason why it was collected in the first place
- Where you have removed your consent for us to use your information (where there is no other legal reason for us to use it)
- Where there is no legal reason for the use of your information
- Where deleting the information is a legal requirement

Where your personal information has been shared with others, we'll do what we can to make sure those using your personal information comply with your request for erasure.

Please note that we can't delete your information where:

- we're required to have it by law
- it is used for freedom of expression
- it is for, scientific or historical research, or statistical purposes where it would make information unusable
- it is necessary for legal claims

You can ask to limit what we use your personal data for

You have the right to ask us to restrict what we use your personal information for where:

- you have identified inaccurate information, and have told us of it
- where we have no legal reason to use that information but you want us to restrict what we use it for rather than erase the information altogether

When information is restricted it can't be used other than to store securely the data and with your consent; or, to handle legal claims and protect others, or where it's for important public interests of the UK.

Where restriction of use has been granted, we'll inform you before we carry on using your personal information.

You have the right to ask us to stop using your personal information for any service we provide. You also have the right to unsubscribe from any materials we may send you. However, if you make a request this may cause delays or prevent us delivering services to you.

Where possible we'll seek to comply with your request, but we may need to hold or use information because we are required to by law or by contract.

If you wish to contact us with respect to these matters please contact the Data Protection Officer on 0844 745 2001

You can ask to have your information moved to another provider (data portability)

You have the right to ask for your personal information to be given back to you or another service provider of your choice in a commonly used format. This is called data portability.

However, this only applies if we're using your personal information with consent (not if we're required to by law).

You can ask to have any 'computer-made' decisions explained to you, or choose not to be the subject of a decision which is based on automated processing. You have the right to question decisions made about you by a computer, unless it's required for any contract you have entered into, required by law, or you've consented to it.

You also have the right to object if you are being 'profiled'. Profiling is where decisions are made about you based on certain things in your personal information, e.g. your health conditions.

If GSS uses your personal information to profile you, to deliver the most appropriate service to you, you will be informed.

If you have concerns regarding automated decision-making, or profiling, please contact the Data Protection Officer on 0844 745 2001 who'll be able to advise you about how we are using your information.

Who do we share your information with?

We use a range of organisations to either store personal information or help deliver our services to you. Where we have these arrangements, there is always an agreement in place to make sure that the organisation complies with data protection law.

Sometimes we have a legal or contractual duty to provide personal information to other organisations. This may be because we need to give that data for legitimate business purposes. We may also need to give that information to the courts for legal purposes.

We may also share your personal information when we feel there's a good reason that's more important than protecting your privacy. This doesn't happen often, but we may share your information:

- to find and stop crime and fraud; or
- if there are serious risks to the public, our staff or to other professionals;
- to protect a child; or
- to protect adults who are thought to be at risk, for example if they are frail, confused or cannot understand what is happening to them

For all of these reasons the risk must be serious before we can override your right to privacy.

If we're worried about your physical safety or feel we need to take action to protect you from being harmed in other ways, we'll discuss this with you and, if possible, get your permission to tell others about your situation before doing so.

We may still share your information if we believe the risk to others is serious enough to do so.

There may also be rare occasions when the risk to others is so great that we need to share information straight away. If this is the case, we'll make sure that we record what information we share and our reasons for doing so. We'll let you know what we've done and why if we think it is safe to do so.

How do we protect your information?

We'll do what we can to make sure we hold records about you (on paper and electronically) in a secure way, and we'll only make them available to those who have a right to see them. Examples of our security include:

- Encryption, meaning that information is hidden so that it cannot be read without special knowledge (such as a password). This is done with a secret code or what's called a 'cypher'. The hidden information is said to then be 'encrypted'
- Controlling access to systems and networks allows us to stop people who are not allowed to view your personal information from getting access to it
- Training for our staff allows us to make them aware of how to handle information and how and when to report when something goes wrong
- Regular testing of our technology and ways of working including keeping up to date on the latest security updates

You can find more details of our Information Security expectations on our online policy.

Where in the world is your information?

The majority of personal information is stored on systems in the UK. But there are some occasions where your information may leave the UK either in order to get to another organisation or if it's stored in a system inside the EU.

We have additional protections on your information if it leaves the UK ranging from secure ways of transferring data to ensuring we have a robust contract in place with that third party.

We'll take all practical steps to make your personal information is not sent to a country that is not seen as 'safe' either by the UK or EU Governments.

We will only keep your information for as long as we need it

We will retain your personal information only for as long as we need it in order to fulfil the purposes for which we have initially collected it, unless otherwise required by law or contractual requirements.

Paperwork - Our office environment

All GSS staff are responsible for ensuring the security for all documents containing confidential information about Clients and or customers wherever and however this may have been come by or have arisen. This covers all communication, paperwork pertaining to customers and information containing customer, client or staff personal information.

All files and paperwork containing any of the above information will be kept locked in secure cabinets (except when in use) and accessible by delegated key holders only.

Electronic Information

E-mails containing confidential information should not be sent unless we are confident that the relevant person will receive them internally or externally and will be flagged as confidential. Any information concerning personal information can only be forwarded on with permission of those concerned only. All emails pertaining to GSS work must be routed via GSS own email address and must always comply with GSS *Internet usage policy* and *Information and Data Security policy*.

Multiple Customer Emails

Where a single email is to be sent out to more than 2 unknown customers simultaneously the following procedures must be adhered to:

1. Customer email addresses must be collated from spreadsheets / information provided by GSS Management only
2. No more than 30 emails should be mailed at any one time in a single email mail out
3. Once the email has been constructed it must be double checked by a second Team member
4. All emails MUST BE SENT using the BCC function only
5. Emails must be fully checked prior to sending by a member of GSS Management Team to ensure that the email is
 - a. Using bcc only as the send function
 - b. it is grammatically correct
 - c. It meets all GSS guidelines for emailing customers and does not contain any sensitive data

Electronically held data

All information held electronically containing sensitive information will be held under pass-word protected files. Customer records are held on our own database through our own server with data only required for the purpose of the work at the time. GSS server is held in a secure manned office (this is locked when not manned) and is within an alarmed area of the premises. All data is backed up internally and daily back up tapes are only removed from the premises overnight.

Confidential data no longer in use or outdated/invalid will be held securely for a maximum of 12 months after the last usage at which point will be securely destroyed or disposed of unless by prior arrangement from GSS business, partners, contractors or other.

All electronically held data must also comply with GSS *GDPR and Information and Data Security Policy*.

Third Party Data

Information received via any third party which may include sensitive data, such as customers Date of Birth, National Insurance details or any identifying information must under no circumstances be emailed, or faxed to any other organisation or party without prior consent of the named individuals to which the data concerns. In-formation that needs to be passed to relating bodies (only) for verification can only be done through secure methods.

Where can I get advice?

If you have any worries or questions about how your personal information is handled please contact our Data Protection Office, the details of which are at the top of this page.

For independent advice about data protection, privacy and data sharing issues or if you would like to make a complaint if you think we have done something wrong with the data we hold about you, you can contact the Information Commissioner's Office (ICO) at:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF

Alternatively, visit www.ico.org.uk or email casework@ico.org.uk

Changes to our Privacy Statement

From time to time we may make changes to this privacy statement. Any changes be posted on this website so you are always aware of what information we collect, how we use it, and under what circumstances, if any, we disclose it. If at any time we decide to use personal data in a manner significantly different from that stated in this privacy statement, or otherwise disclosed to you at the time it was collected, we will notify you by email, and you will have a choice as to whether or not we use your information in the new manner.

Links to other websites

Our website may contain links to other websites of interest. However, once you have used these links to leave our site, you should note that we do not have any control over other websites. Therefore, we cannot be responsible for the protection and privacy of any information which you provide whilst visiting such sites and such sites are not governed by this privacy statement. You should exercise caution and look at the privacy statement applicable to the website in question.

Review

This policy will be reviewed and updated as necessary to reflect best practice, future amendments to relevant acts and or changes in legislation or GSS's policies and procedures

Any breaches to the above could constitute gross misconduct and where found, individuals could be subject to disciplinary procedures accordingly.

This policy is not exhaustive and is in conjunction with GSS Information and Data Security, General Data Protection Policy and Confidentiality.



Signed by Sonia Benjamin
Director
15.07. 2019
Updated v2