

Data Privacy Policy:

Introduction.

Your privacy is important to us, so we've developed a Privacy Policy that covers how we collect, use, disclose and store your personal information. Please take a moment to familiarize yourself with our privacy policy and contact us if you have any questions.

Who we Are:

We are a national supplier providing services, as set out on our website, to the facilities and premises owned by our clients.

How We Use Your Information:

This privacy notice tells you what to expect when Anchor Security Services Ltd, T/a Anchor Group Services, and Ocean Parking collects personal information. Anchor Security Services is the controller for the personal information we process, unless otherwise stated. It applies to information we collect about:

- People who use our services, e.g., who subscribe to our newsletter or request a publication from us.
- Visitors to our website.
- Job applicants and our current and former employees.
- Complainants and other individuals in relation to a data protection complaint or enquiry.
- Individuals tracked via GPS Systems in relation to the use of company assets or for operational purposes.
- Motorists parking on private land. ANPR cameras and, or attendants to capture your vehicle registration mark for the purposes of Car Park Management and Enforcement. Your data may be collected, processed, retained, and shared in order to enforce the parking contract and protect legitimate interests in the following ways:
 - Disclosed to or requested from the DVLA.
 - Payment information for PCNs.
 - Shared with third parties in relation to the issue of a Parking Charge Notice in order to assist with appeals, collect sums due or to conduct legal proceedings.
 - Shared with the police or security organisations to prevent or detect crime.
 - Shared with organisations for statistical analysis.
- CCTV footage from both Body Worn Cameras and CCTV Systems (E-Guarding) and or whilst managing and operating CCTV Systems on behalf of Anchor and or its clients.

Why Do We Use Your Information?

We will only use your personal information when the law allows us to do so. Most commonly, we will use your personal information in the following circumstances:

- Where we need to perform a contract, we have entered into with you.
- Where we need to comply with a legal obligation.
- Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.
- To protect your interests (or someone else's interests) or where it is needed in the public interest although these circumstances are likely to be rare.

Specific examples of ways in which we may use your personal information include:

Customer Administration. We may use information about you including form information, content, and other information you provide to us or which we collect about you as necessary to carry out our contracts with you, and for our legitimate interests in administering your account.

Direct Marketing. We may send direct postal or electronic marketing to you using your contact details and information you have provided us. We use this as necessary for our legitimate interests in marketing to you and maintain a list of potential customers. If you are not acting as a business and have not provided your contact details directly to us in relation to our products, we will only

send electronic marketing to you if you have consented to that marketing. We will always provide an “opt-out” option on any marketing messages we send you.

Operational use of GPS Data. We may collect GPS Tracking data for company- issued devices or vehicles to ensure operational efficiency, employee safety, and compliance with applicable laws and regulations.

Third Party Personnel Administration. If you work for one of our customers or suppliers, we may hold information on you. This includes information you provide when you correspond with us, as well as details of your employment, contact details, and our relationship with you. We use this as necessary for our legitimate interests in managing our relationship with your employer.

Job Applications. If you apply for a position with us, we hold and use information on you. This will include information you provide to us in your application, as well as opinion information on you from any referees you provide. We may also obtain criminal record and identity verification information from reference agencies. We use this as necessary to enter into an employment contract with you, and for our legitimate interests in evaluating candidates and recording our recruitment activities, and as necessary to exercise and perform our employment law obligations and rights.

Former Employees. If you used to work for us, your information will be used in accordance with our employee privacy notice. If you are a former employee or contractor and require a copy of this, please contact us.

We will only use your personal information for the purposes for which we collected it as set out in this notice, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Visitors to Our Websites:

When someone visits www.anchorgroupservices.co.uk we use a third-party service, Google Analytics, to collect standard internet log information and details of visitor behaviour patterns. We do this to find out things such as the number of visitors to the various parts of the site. This information is only processed in a way which does not identify anyone. We do not make, and do not allow Google to make any attempt to find out the identities of those visiting our website.

Information about our Use of Cookies:

Our website uses cookies to distinguish you from other users of our website. This helps us to provide you with a good experience when you browse our website and also allows us to improve our site.

What is a Cookie:

A cookie is simply a technology for remembering something about you.

Without cookies, a website is like a goldfish who loses its memory every time you visit a new page. Once you visit a new page, it doesn't remember who you are.

Now this can be a good and a bad thing. Without any memory, a website can't do a lot of stuff. It can't let you log in because it forgets who you are. It can't let you buy anything because it forgets what you're buying. But it also means it can't track you. Some websites use cookies to remember what you do on their website, and to target ads at you and some of those websites share their cookies, so that ads on one website know what you liked on another. This has scared a lot of people.

Cookies aren't automatically good or bad, but it's worth understanding what you can do about them. You can turn them off completely, which is a bit like banning all music to prevent another Justin Bieber album. Many websites simply won't work.

A better option would be to turn off 3rd party cookies, which will stop most websites from sharing information about you. Some browsers – like Safari – do this automatically.

And finally, you can take a deeper look into any websites which concern you. Most websites have policies that explain what they do if you care to look.

E-Newsletter:

We use a third-party provider, Zoho Campaigns, to deliver our monthly e-newsletters. We gather statistics around email opening and clicks using industry standard technologies including clear gifs to help us monitor and improve our e-newsletter. For more information, please see <https://www.zoho.com/campaigns>

People who contact is through Social Media:

If you send us a direct message via social media, the message will be stored for six months and then deleted. It will not be shared with any other organisation.

People who Email us:

We will also monitor any emails sent to us, including file attachments, for viruses or malicious software. Please be aware that you have a responsibility to ensure that any email you send is within the bounds of the law.

What Data We Collect:

In connection with the different ways, we may interact with you and the various services that we provide, we collect the following categories of data:

- Contact information, including name, address, telephone number and e-mail address.
- Identity data, including gender and date of birth.
- Vehicle registration details captured by ANPR cameras and/or attendants.
- Communication data between you and us, including recordings of calls to our head office and control room, e-mail communication, comments and reviews collected through surveys or posted on our channels and on social media platforms.
- Digital information data collected when you visit our websites, applications, or other digital platforms, including IP-addresses, browser data, traffic data, social media behaviour, and user patterns. If you subscribe to our newsletters, we may collect data regarding which newsletters you open, your location when opening them and whether you access any links inserted in the newsletters.

Use of Third-Party Processors:

We use third party data processors to provide elements of our service. We have processing agreements in place with these companies. This means that they cannot do anything with your personal information unless we have instructed them to do it. They will not share your personal information with any organisation apart from what is agreed with us. They will hold it securely and retain it for the period we instruct.

Who we share your data with:

We may share your data with the following.

- The Payment Processor for processing any online payments,
- The Driver Vehicle Licensing Agency (DVLA),
- The Parking on Private Land Appeals (POPLA) Service or the Independent Appeals Service (IAS) for the purpose of assessing any appeals,
- Print and mail service providers for the purpose of contacting you by post,
- Email service providers for the purpose of responding to you once you have consented by email,
- If you have not replied to other correspondence, we may share your data with third party collection processors and/or solicitors for the purpose of enforcing a parking contract or responding to a legal query,
- Any other duly authorised sub-contractors,
- HMRC.
- The Police, Security Services, and or enforcement agencies.

Sensitive Personal Data:

You may voluntarily share sensitive personal data to us via telephone calls, letters, or emails, but we will never ask for this information.

Recorded Phone Call:

We may monitor and/or record phone calls between administration staff and you in order to assist in providing both you and our staff additional security, to help resolve complaints and for overall training and quality purposes.

Job applicants, current and former Anchor Group Services employees:

Anchor Group Services is the data controller for the information you provide during the process of application, employment and leaving the Company unless otherwise stated.

What we will do with the information you provide us:

All of the information you provide during the process will only be used for the purpose of progressing your application, or to fulfil legal or regulatory requirements as necessary during your employment. We do not collect more information than we need to fulfil our stated purposes and will not retain it for longer than is necessary.

The information we ask for is used to assess your suitability for employment. You don't have to provide what we ask for, but it might affect your application if you don't. We will not share any of the information you provide during the recruitment process or your employment with any third parties for marketing purposes or store any of your information outside of the European Economic Area. The information you provide will be held securely by us and/or our data processors whether the information is in electronic or physical format.

We will use the contact details you provide to us to contact you to progress your application. We will use the other information you provide to assess your suitability for the role you have applied for. Should you be successful we will use the information to schedule, manage and pay you.

How we make decisions about recruitment:

Final recruitment decisions are made by hiring managers and members of our recruitment team. All of the information gathered during the application process (apart from equal opportunities data) is taken into account.

You are able to ask about decisions made about your application by speaking to your contact within our recruitment team or by emailing - hr@anchorgroupservices.co.uk

What information do we ask for, and why?

We do not collect more information than we need to fulfil our stated purposes and will not retain it for longer than is necessary. The information we ask for is used to assess your suitability for employment. You don't have to provide what we ask for, but it might affect your application if you don't.

Application Stage:

We ask you for your personal details including name and contact details. We will also ask you about your previous experience, education, referees and for answers to questions relevant to the role you have applied for. Our recruitment team and recruiting managers will have access to all of this information to make the decision.

You will also be asked to provide equal opportunities information. This is not mandatory information – if you don't provide it, it will not affect your application. This information will not be made available to any staff outside of our recruitment team, including hiring managers, in a way which can identify you. Any such information you do provide, will be used only to produce, and monitor equal opportunities statistics.

Shortlisting:

Our hiring manager's read and then shortlist applications for interview. They may be provided with your name and/or contact details but will not be provided with your equal opportunities information if you have provided it.

Assessments:

We might ask you to participate in assessment days. complete tests or occupational personality profile questionnaires. and/or attend an interview – or a combination of these. Information will be

generated by you and by us. For example, you might complete a written test, or we might take interview notes. This information is held by Anchor Group Services.

If you are unsuccessful following an assessment for the position you have applied for, we may ask if you would like your details to be retained in our talent pool for a period of three months. If you say yes, we may contact you should any further suitable vacancies arise.

Conditional Offer:

If we make a conditional offer of employment, we will ask you for information so that we can carry out pre-employment checks. You must successfully complete pre-employment checks to progress to a final offer. We are required to confirm the identity of our staff, their right to work in the United Kingdom and seek assurance as to their trustworthiness, integrity, and reliability.

You will therefore be required to provide:

- Proof of your identity – you will be asked to attend a designated site with original documents, which we will take copies of.
- Proof of your qualifications – you will be asked to attend a designated site with original documents, which we will take copies of.
- You will be asked to complete a criminal records declaration to declare any unspent convictions.
- We will contact your referees, using the details you provide in your application, directly to obtain references.
- We will also ask you to complete a questionnaire about your health. This is to establish your fitness to work.

If we make a final offer, we will also ask you for the following:

- Bank details – to process salary payments.
- Emergency contact details – so we know who to contact in case you have an emergency at work.
- Your eligibility for or Membership of a Civil Service or Local Authority Pension scheme – so we can send you a questionnaire to determine whether you are eligible to re-join your previous scheme.

Use of Data Processors:

Data processors are third parties who provide elements of our recruitment service for us. We have contracts in place with our data processors. This means that where we have contracted them, they cannot do anything with your personal information unless we have instructed them to do it. They will not share your personal information with any organisation apart from us. They will hold it securely and retain it for the period we instruct. We do use other third parties and subscribe to their privacy terms and would expect you to do so too so that we can effectively process your application. One such arrangement is with Indeed Jobs.

How long is the information retained for?

If you are successful, the information you provide during the application process will be retained by us as part of your employee file for the duration of your employment plus 6 years following the end of your employment. This includes your, fitness to work, records of any security checks and references.

If you are unsuccessful at any stage of the process, the information you have provided until that point will be retained for up to a maximum of 6 months from the closure of the campaign.

Information generated throughout the assessment process, for example interview notes, is retained by us for no more than 6 months following the closure of the campaign.

Equal opportunities information is retained for 6 months following the closure of the campaign whether you are successful or not.

How we make decisions about recruitment:

Final recruitment decisions are made by hiring managers and members of our recruitment team. All of the information gathered during the application process (apart from equal opportunities data) is taken into account.

You are able to ask about decisions made about your application by speaking to your contact within our recruitment team or by emailing – hr@anchorgroupservices.co.uk

Disclosure of personal information:

Being mindful of our responsibilities when processing personal data in many circumstances we will not disclose personal data without prior consent, however when we investigate a complaint or are asked for data by an official agency, for example, we may need to share personal information with the organisation concerned and with other relevant bodies who have the right to request personal data in such circumstances.

Access to personal data and complaints:

Under data protection law, you have the following rights in respect of the information we hold about you.

Access:

You are entitled to access the information which we hold about you. In order to protect your information, we may request that you provide evidence of your identity such as a photocopy (please do not send us the original) of your current passport or driving licence.

Rectification:

If you do not think that the information we hold about you is correct, or you think that we do not have all the information which we should have about you, you can request that we rectify this information.

Restriction:

You can ask that we restrict the way that your data is used. This means that we will store your data securely, but it will not be processed anymore.

Object:

If you object to the way that we are processing your data, you can contact us to tell us why you think we should stop processing it.

Erasure:

Once we have finished processing your data you can request that we erase the data which we hold about you.

Respond:

Once we have received your request for us to do any of the above, we will contact you within one calendar month either to confirm that we have carried out your request or why we have not. In some cases, we will not have to process your request, or will not be able to. We will still contact you within 30 days (28days for February) to explain to you why this is the case.

Complaints:

If you wish to raise a complaint about how your data has been handled, there are many ways you can contact us including.

By phone: 01244 354700.

By email: DPO@anchorgroupservices.co.uk

And by post: Data Protection Officer, Anchor Security Services, Carlton House, Chester Business Park, Chester, Cheshire. CH4 9QE.

If you are not satisfied with our resolution of your concern, then please contact the Information Commissioner's Office on 0303 123 1113.

Other Websites:

Our site may, from time to time, contain links to and from the websites of third parties. If you follow a link to any of these websites, please note that these websites have their own privacy policies and that we do not accept any responsibility or liability for these policies or your use of those websites.

Changes to our Privacy Notice:

Any changes we may make to our privacy policy in the future will be posted on this page and we suggest that you check back frequently to see any updates or changes to our privacy policy.

This privacy notice was last updated June 2024.

Associated Documentation:

Version	Description of Documentation
	AGS HL Po 003 – Social Media Policy.
	AGS HL Po 003a – Group Chat and Messenger Usage Policy.
	AGS HL Po 009 – General Data Protection Regulations (GDPR) Policy
	AGS HL Po 021 Information Security Policy.
	AGS HL Po 023 – Information Technology Adoption & Usage Policy.
	AGS HL Po 025 Subject Access Request (SAR) Policy.
	AGS HL Pr 022 Subject Access Request (SAR) Procedure.
	AGS HL Pr 023 Data Breach Reporting Procedure.

Legal Disclaimer:






All material contained within this document is confidential information and the document and any attachments may be legally privileged. Dissemination, copying, changing or other use of its content is strictly prohibited and may be unlawful. Any changes required in regards the contents and or structure of this document are to be notified to the H.R Department and HSEQ Manager prior to any changes being authorised and will only be made under the organisation's Change Control Procedure. If you are not on the intended recipient(s) list, please inform Anchor Group Services Limited's H.R Department. No contract may be construed from this document.

Amendment Log

Reason for Review	Details of Change	Verified by:	Date:
HR Amendments	Addition of monitoring Points,	Sue Tait	01/12/24

Document Review Date

[Date of review (default is 12 months from creation / last review unless there is a significant change in company policy).

Reason for Review:	Name:	Signature:	Date:
Created.	Andrew Harper (CEO).		01.07.2017
Review.	Andrew Harper (CEO)		01.10.2018
Review.	Andrew Harper (CEO).		01.10.2019
Review.	Andrew Harper (CEO).		01.10.2020
Review.	Andrew Harper (CEO).		01.10.2021

Review.	Andrew Harper (CEO).		01.10.2022
Review.	Andrew Harper (CEO).		01.10.2023
Review.	Andrew Harper (CEO).		01.10.2024
Review.			01.10.2025

Acknowledgement.

I have read and understood the contents of this document (AGS HL Po 009a Data Privacy Policy). Anything I did not understand has been explained to me to my satisfaction.

Print Name:	Signed:	Date: