Data Protection and Privacy Policy

This Policy is effective as of 30/09/2025.

This Policy is due for review on 30/09/2026.

1. Introduction

This policy applies to Amber Valley School Sport Partnership CIO (AVSSP) products, services, content, features, technologies, functions, contact (including e-mail), websites and mobile applications.

This policy outlines the expected behaviour of us, our employees and third-parties in relation to the collection, use, retention, transfer, disclosure and erasure of any personal data belonging to you.

Unless indicated otherwise, this Policy doesn't apply to third party products or services. It also doesn't apply to the practices of companies that we don't own or control, including other companies you might interact with when using the Services.

If you have any comments on this Policy, please contact us by visiting https://www.avssp.co.uk/contact.

2. Definitions and key terms

Data

Data means information which:

· is being processed by means of equipment operating automatically in response to instructions given for that purpose,

· is recorded with the intention that it should be processed by means of such equipment,

· is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system; or

· is recorded information held by a public authority.

Data Subject

Data Subject means an individual who is the subject of personal data. We may also use "you", "your" and "yours" to describe Data Subjects in this Policy.

Data Controller

Data controller means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

Data Protection Act (DPA)

The Data Protection Act 2018.

Data Protection Officer (DPO)

The Data Protection Officer (DPO) is responsible for matters relating to privacy and data protection.

Employees

All employees, staff and volunteers.

Form

A Form includes any of the following that exist on the Services:

- surveys,
- contact forms,
- newsletter subscriptions forms,
- user registrations forms,
- e-commerce forms,
- other registration forms; and
- text boxes.

General Data Protection Regulation (GDPR)

The General Data Protection Regulation (Regulation (EU) 2016/679).

Personal Data

Personal Data is any information (including opinions and intentions) which relates to an identified or Identifiable Natural Person.

Policy

This Data Protection and Privacy Policy.

Processing

Processing, in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:

· organisation, adaptation or alteration of the information or data,

· retrieval, consultation or use of the information or data,

· disclosure of the information or data by transmission, broadcast or otherwise making available; or

· alignment, combination, blocking, erasure or destruction of the information or data.

Sensitive Personal Data

Sensitive personal data includes:

- data relating to medical information,
- gender,
- religion,
- race,
- sexual orientation,
- trade union membership; and
- criminal records and proceedings.

Services

The Services include our:

- products,
- services,
- content,
- features,
- technologies,
- functions,
- contact (including e-mail),
- websites; and
- mobile applications.

Our websites include:

- avssp.co.uk,
- ozzys-adventures.co.uk,
- dtffitness.co.uk,
- dothinkfeelpe.co.uk; and
- spwa.co.uk.

Third-Party Data Processors

Third parties involved in the processing of Personal Data. These Third-Party Data Processors may include:

- digital agencies,
- hosting providers,
- data storage providers; and
- other technical partners.

We, us and our

Amber Valley School Sport Partnership

3. Who we are

The Services are operated by Amber Valley School Sport Partnership, a Charitable Incorporated Organisation, registered in England.

Some important details about us:

Our business address is: AVSSP, Swanwick School & Sports College, Hayes Lane, Swanwick, DE55 1AR

Our registered address is: AVSSP, Swanwick School & Sports College, Hayes Lane, Swanwick, DE55 1AR

Our charity number is: 1162691

Responsibilities

Our Board / directors have overall responsibility to make sure that we comply with our legal obligations.

Our Data Protection Officer is responsible for:

- briefing the Board / our directors on Data Protection obligations,
- reviewing Data Protection and related policies,
- advising other staff on tricky Data Protection issues,
- ensuring that Data Protection induction and training takes place,
- informing the ICO,
- handling subject access requests,
- approving unusual disclosures of personal data; and
- approving contracts with Data Processors.

Our department heads and managers are responsible for monitoring their own, and their teams, compliance with GDPR. They are also responsible for reporting back to the Data Protection Officer.

All Employees are required to read, understand and accept all of our policies and procedures.

4. Details of the Data Controller

An organisation that handles Personal Data and makes decisions about its use is known as a Data Controller. We process Personal Data both as the Data Controller and a Data Processor. Here are the details for the Data Controller:

Amber Valley School Sport Partnership (AVSSP)

Business Address:
AVSSP, Swanwick School & Sports College, Hayes Lane, Swanwick, DE55 1AR

Registered Address:
AVSSP, Swanwick School & Sports College, Hayes Lane, Swanwick, DE55 1AR

Phone: 07766398562

Website: https://www.avssp.co.uk
E-mail: info@avssp.co.uk

5. Details of the Data Protection Officer

The Data Protection Officer (DPO) is responsible for matters relating to privacy and data protection. Here are the contact details for the DPO:

Amber Valley School Sport Partnership (AVSSP)

Business Address:
AVSSP, Swanwick School & Sports College, Hayes Lane, Swanwick, DE55 1AR

Registered Address:
Robert Shaw, Swanwick School & Sports College, Hayes Lane, Swanwick, DE55 1AR

Phone: 01773 417204

Website: https://www.avssp.co.uk
E-mail: info@avssp.co.uk

6. Data protection principles

We're committed to processing data in accordance with our obligations under the GDPR and the DPA. Article 5 of the GDPR requires that Personal Data shall be:

- processed lawfully, fairly and in a transparent manner,
- collected and processed for specified, explicit and legitimate purposes,
- adequate, relevant and limited to what's necessary in relation to the purposes for which they're processed,
- accurate and kept up to date,
- erased or rectified without delay if inaccurate,
- kept in a form which permits identification of Data Subjects for no longer than is necessary; and
- processed in a manner that ensures appropriate security of the personal data,

7. Lawful, fair and transparent processing

To ensure our processing of data is lawful, fair and transparent, we shall maintain:

- an Information Asset Register,
- an IT Equipment Asset Register,
- Audit Trail Logs,
- a File Classification Policy; and
- Retention Schedules.

These systems and policies shall be reviewed at least annually.

All data that we process must be done on one of the following lawful bases:

- consent,
- contract,
- legal obligation,
- vital interests,
- public task; or
- legitimate interests.

We shall note the appropriate lawful basis in the Information Asset Register.

If we use consent for processing data, evidence of this shall be kept with the personal data. Also, if we contact you, the option for you to revoke your consent will be clearly available. Systems are in place to ensure such revocation is reflected accurately in our systems.

8. Compliance audits

The DPO will carry out an annual Data Protection compliance audit. Each audit will, as a minimum, assess:

- Compliance with this Policy in relation to the protection of Personal Data, including:
    - The assignment of obligations.
    - Raising awareness.
    - Training of Employees.
- The capability of Data Protection related operational practices, including:
    - Data Subject rights.
    - Personal Data transfers.
    - Personal Data incident management.
    - Personal Data complaints handling.
- The level of awareness of Data Protection policies and Privacy Notices.
- The currency of Data Protection and Privacy policies and Privacy Notices.
- The accuracy of Personal Data being stored.
- The conformity of Data Processor activities.
- The adequacy of procedures for redressing poor compliance and Personal Data Breaches.

The DPO, in cooperation with key stakeholders will plan and schedule the correction of any identified deficiencies within a reasonable time frame. Any major deficiencies identified will be reported to and monitored by our Board / our directors.

9. Data we may collect and how we use your data

The following section explains the data that we may collect, use, how we may categorise it and how we may use the data that we collect.

We only use your Personal Data for the purposes for which you provided it to us, as indicated to you at the time you provided your Personal Data.

We don't identify people to our advertisers, but we do give them aggregate information to help them reach their target audience. We may use information we've collected to display advertisements to that audience.

We don't use Personal Data to automatically profile those who access the Services.

We shall take reasonable steps to ensure personal data is accurate. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

Personal Data we may collect and use from visitors

Anyone who accesses the Services is categorised as a visitor. As a visitor, we may collect and process your data which may include your IP address, use of cookies, pageview activity, frequency of access, geo-location data, time spent on the Services, browser type and version, operating system, device hardware and software versions, device sensor information, data from your camera and photos, connection speed, internet service provider, interaction through social media such as your "likes" of our pages, location from which you accessed the Services, date and time information, page clicks and the length of time you've spent on the Services.

Data collected from visitors is collected automatically through Google Analytics and the use of cookies. We may process this data to provide products and services that you request, provide (with your consent) products and services which we think may interest you, allow you to use our interactive services, deliver, customise and optimise the content and advertisements of the Services, administer the Services, databases, applications and systems, report aggregated information to our advertisers, provide information as required by law in the case of criminal activity, communicate with you, provide support for our products and services, obtain feedback on the level of the Services, keep the Services safe and secure, protect against fraud, spam and abuse and help prevent security breaches.

This data is collected and processed anonymously and when processing this data, we don't draw any conclusions about you. In addition, this data is stored separately from all Personal Data that you provide to us.

We process data collected from visitors on the lawful basis of a legitimate interest in accordance with the GDPR and the DPA.

By accessing the Services, you consent to the collection and use of your Personal Data as described in this Policy. If you don't agree with the terms set out in this Policy, please don't visit or access the Services. If required by applicable law, we'll seek your explicit consent to process Personal Data.

If you choose to withhold Personal Data requested by us, it may not be possible for you to gain access to certain parts of the Services. Withholding Personal Data may prevent us from responding to your queries.

Personal Data we may collect and use from visitors using Forms

Anyone who accesses the Services and puts information into Forms is categorised as a visitor using Forms. In addition to the data we collect for visitors, we may collect and process your Personal Data including your first and last name, postal address, e-mail address, telephone number, employer or company, job title, areas of interest, data retrieved from social networks, publicly available information retrieved from social media, transaction information and a record of any contact between us.

This Personal Data is collected from information you've provided to us by putting information into Forms.

As a visitor using Forms, we process your data on the lawful basis of a legitimate interest in accordance with the GDPR and the DPA.

By putting information into Forms, you consent to the collection and use of your Personal Data as described in this Policy. You also accept that this information could make you personally identifiable to us, our users and the Data Controller.

If you don't agree with the terms set out in this Policy, please don't use forms on the Services. If required by applicable law, we'll seek your explicit consent to process Personal Data.

Personal Data we may collect and use from visitors applying for a job

Anyone who applies for a job at our organisation and provides information to us is categorised as a visitor applying for a job. In addition to the data we collect for visitors and visitors using Forms referenced above, we may collect and process your Personal Data including your employment history and CV.

This Personal Data is collected from information you've provided to us. You may have provided this by completing a Form on the Services or by sending an e-mail to us.

As a visitor applying for a job, we process your data on the lawful basis of a legitimate interest in accordance with the GDPR and the DPA.

We may collect and process the Personal data of applicants to our job listings for the purpose of the processing of the application procedure. The processing may also be carried out electronically. This is the case, in particular, if an applicant submits corresponding application documents by e-mail or by means of a web form on the Services. If an applicant is successful, the data submitted along with the completed employment contract will be stored for the purpose of processing the employment relationship in compliance with legal requirements. If an applicant is unsuccessful, the application documents shall be automatically deleted two months after notification of the refusal decision. We may store data for longer if there are legitimate reasons to, such as a burden of proof in a procedure under the General Equal Treatment Act.

By sending information to us in relation to a job application you may be disclosing information that could make you personally identifiable to us, Third-Party Data Processors and the Data Controller. This also applies to any information you put into job application forms on the Services.

Personal Data we may collect and use from newsletter subscribers

Anyone who subscribes to our newsletter using a form on the Services is categorised as a newsletter subscriber. In addition to the data we collect for visitors and visitors using Forms referenced above, we may collect and process

your Personal Data including your first and last name, e-mail address and communication preferences.

This Personal Data is collected from information you've provided to us by subscribing to our newsletter using a form on the Services. In addition to the ways we process data for visitors and visitors using Forms, we may process your data to let (with your consent) Third-Party Data Processors contact you about other goods and services that might interest you, process your registration to our newsletter and administer our newsletter.

As a newsletter subscriber, we process your data on the lawful basis of consent in accordance with the GDPR and the DPA.

By putting information into our newsletter subscribe forms on the Services, you consent to the collection and use of your Personal Data as described in this Policy. If you don't agree with the terms set out in this Policy, please don't use our newsletter subscribe forms on the Services. If required by applicable law, we'll seek your explicit consent to process Personal Data.

By subscribing to our newsletter, you may be disclosing information that could make you personally identifiable to us, Third-Party Data Processors and the Data Controller.

Personal Data we may collect and use from users

Anyone who registers to the Services is categorised as a user. In addition to the data we collect for visitors, visitors using Forms and newsletter subscribers referenced above, we may collect and process your Personal Data including your password, information about payments, other enrolment information, other profile information and communication preferences.

This Personal Data is collected from information you've provided to us. You may have provided this by putting information into a Form, account section or profile section on the Services.

Where reasonably possible, we'll store your user Personal Data as pseudonymous or encrypted data. Pseudonymisation is a data management procedure by which personally identifiable information fields are replaced by one or more artificial identifiers.

As a user, in addition to the ways we process data for visitors and visitors using Forms, we may process your data to carry out our contracts with you, let (with your consent) Third-Party Data Processors contact you about other goods and services that might interest you, offer you concerned contents or services that may only be offered to registered users and process your registration to the Services.

As a user, we process your data on the lawful basis of consent in accordance with the GDPR and the DPA.

If you're already user, we'll only contact you electronically about things similar to what was previously sold to you.

If you're a new user, you'll only be contacted if you agree to it.

By registering on the Services, you consent to the collection and use of your Personal Data as described in this Policy. If you don't agree with the terms set out in this Policy, please don't register or login to the Services. If required by applicable law, we'll seek your explicit consent to process Personal Data.

By using, and registering on, the Services as a user, you may be disclosing information that could make you personally identifiable to us, our users, third-parties processors and the Data Controller.

We won't sell or rent your personally identifiable information, gathered as a result of filling out Forms, to anyone.

Personal Data we may collect and use from customers

Anyone who purchases products or services on the Services, is categorised as a customer. In addition to the data we collect for visitors, visitors using Forms, newsletter subscribers and users referenced above, we may collect and process your Personal Data including your products and services and your billing information.

This Personal Data is collected from information you've provided to us by purchasing products or services on the Services. As a customer, in addition to the ways we process data for visitors and users, we may process your data to process payments.

As a customer, we process your data on the lawful basis of contractual necessity in accordance with the GDPR and the DPA.

If you're already our customer, we'll only contact you electronically about things similar to what was previously sold to you.

If you're a new customer, you'll only be contacted if you agree to it.

E-mails

If you choose to send data using e-mail, you accept that e-mails are not secure. You also accept that they cannot be guaranteed to be error free as they can be intercepted, amended, or contain viruses. Anyone who communicates with us by e-mail is deemed to have accepted these risks.

We are not responsible for errors or omissions in e-mail messages. We deny any responsibility for any damage arising from the use of e-mail.

CCTV

We, our landlord or a hired third-party may own and operate a CCTV network for the purposes of crime prevention and detection.

Automated Number Plate Recognition (ANPR) cameras may be used and operated or automated vehicle access.

Where you can be identified, images will be processed as Personal Data.

Personalisation of Services

With your consent, we may use the data you give us to build up a picture of your interests. We may also combine this data with other information we've collected about you.

We may use this data to try to ensure that when you access the Services, you don't miss the offers and information relevant to you. We may also use this data

for the purposes of statistical analysis, sales and marketing research, tracking page usage and paths you use, tailoring the Services, tailoring our marketing campaigns, and tailoring our e-mail communications.

10. Data from children

Children are unable to consent to the processing of Personal Data for the Services. Consent must be sought from the person who holds parental responsibility over the child. However, it should be noted that where processing is lawful under other grounds, consent needn't be obtained from the child or the holder of parental responsibility.

Should we foresee a business need for obtaining parental consent for the Services offered directly to a child, guidance and approval must be obtained from the DPO before any processing of a child's Personal Data may commence.

11. Sensitive Personal Data

We may, from time to time, be required to process Sensitive Personal Data. Sensitive Personal Data includes data relating to medical information, gender, religion, race, sexual orientation, trade union membership and criminal records and proceedings.

We'll only process Sensitive Personal Data if you've expressly consented to such processing or where one of the following conditions apply:

· The processing relates to Personal Data which you've already made public.

· The processing is necessary for the establishment, exercise or defence of legal claims.

· The processing is specifically authorised or required by law.

· The processing is necessary to protect your vital interests or of another natural person where you're physically or legally incapable of giving consent.

· Further conditions, including limitations, based upon national law related to the processing of genetic data, biometric data or data concerning health.

In any situation where Sensitive Personal Data are to be processed, prior approval must be obtained from our DPO. The basis for the processing must be clearly recorded with the Personal Data in question.

Where Sensitive Personal Data are being processed, we'll adopt additional protection measures.

12. Disclosing and sharing your information

We may disclose your information to others in the following cases:

Affiliates and acquirers of our business or assets

We may share your information with affiliates under common control with us, who are required to comply with the terms of this Policy with regard to your information. We may share or transfer your information if we undergo or become involved in the sale of our business, a business combination, securities offering, bankruptcy, re-organisation, dissolution or other similar transactions.

Employees, agents and contractors

We may disclose your information to our offices, other businesses in our group, our agents, our contractors or our contractors' employees. These entities assist us in providing the services we offer and will only use your information to the extent necessary to perform their functions.

Legal obligation

We can also exchange your information with others to protect against fraud or credit risks.

We may share your information with third parties if disclosure is reasonably necessary or appropriate in order to meet legal obligations, protect other people's property, safety or rights, prevent any person from death or serious bodily injury, address issues of national security or other issues of public importance, prevent or detect violations of our Terms of Service, prevent fraud or abuse of us or our users, protect our operations or our property, or protect our legal rights.

These third parties may include law enforcement, public or governmental agencies, or private litigants and may be within or outside your country of residence.

Third-Party Data Processors

We may share your information with Third-Party Data Processors that assist us in: administering the Services, processing data submitted to the Services, providing products and services, support the Services, improve the Services, promote the Services, process payments, fulfil orders, or performing technical operations.

These Third-Party Data Processors will only have access to the information necessary to perform these limited functions on our behalf. They are required to protect and secure your information. We may also engage Third-Party Data Processors to collect information about your use of the Services over time on our behalf. We do this so that we or they may promote us or display information that may be relevant to your interests on the Services or other websites or services. Some of these Third-Party Data Processors may be located outside of the country where you accessed the Services. This information may be shared automatically once you've submitted information to us.

Publicly available information

Subject to your privacy settings, your information and content may be publicly accessible.

DMCA notices

We may share your information with third parties when we forward Digital Millennium Copyright Act (DMCA) notifications. These notifications will be forwarded as submitted to us without any deletions.

13. Details of the Third-Party Data Processors

The following section includes details of Third-Party Data Processors that help us administer, and process data submitted to, the Services. They also help us in providing products and services and perform technical operations. Some of these Third-Party Data Processors may be located outside of the country where you accessed the Services.

Website(s)

Bloobo are responsible for processing your data that may be stored on our website servers and website database for the following websites:

- avssp.co.uk
- pecoordinator.co.uk

Here are the details for the operating company of the website:

Bloobo LTD (Trading name of NSB Services Ltd)

Business Address:
72 Wilson Street, Derby, Derbyshire, England, DE1 1PL

Registered Address:
First Floor, Telecom House, 125-135 Preston Road, Brighton, England, BN1 6AF

Contact Information:
Phone: +44 (0)1332 527 538

Website: https://bloobo.co.uk
E-mail: support@bloobo.co.uk

Data Location(s):
Manchester, England

Derby, England

Data Protection and Privacy Policy:
https://bloobo.co.uk/privacy

Website(s)

UKFast are responsible for processing your data that may be stored on our website servers and website database for the following websites:

- avssp.co.uk
- pecoordinator.co.uk

Here are the details for the operating company of the website:

UKFast.Net Ltd

Business Address:
UKFast Campus, Birley Fields, Manchester, M15 5QJ

Registered Address:
UKFast Campus, Birley Fields, Manchester, M15 5QJ

Contact Information:
Phone: +44 (0)844 576 3950

Website: https://www.ukfast.co.uk

Data Location(s):
United Kingdom

Data Protection and Privacy Policy:
https://www.ukfast.co.uk/terms/privacy-policy.html

Mobile Application(s)

Bloobo are responsible for processing your data that may be stored on our mobile application servers and database.

Here are the details for the operating company of the mobile application:

Bloobo (Trading name of NSB Services Ltd)

Business Address:
72 Wilson Street, Derby, Derbyshire, England, DE1 1PL

Registered Address:
First Floor, Telecom House, 125-135 Preston Road, Brighton, England, BN1 6AF

Contact Information:

Phone: +44 (0)1332 527 538

Website: https://bloobo.co.uk
E-mail: support@bloobo.co.uk

Data Location(s):
Manchester, England

Derby, England

United States

Data Protection and Privacy Policy:
https://bloobo.co.uk/privacy

IT Systems

Microsoft are responsible for processing your data that may be stored on our IT systems.

Here are the details for the operating company of the IT systems:

Microsoft Limited

Business Address:
Microsoft Campus, Thames Valley Park, Reading, Berkshire, England, RG6 1WG

Registered Address:
Microsoft Campus, Thames Valley Park, Reading, Berkshire, England, RG6 1WG

Contact Information:

Phone: +44 (0)344 800 2400

Website: https://www.office.com

Data Location(s):
Durham, England

London, England

Cardiff, Wales

Data Protection and Privacy Policy:
https://www.microsoft.com/en-us/trustcenter/privacy/

Google Analytics

We've integrated the component of Google Analytics (with Anonymisation function) with the Services. Google Analytics is a Web Analytics service. Web Analytics is the collection, gathering and analysis of data about the behaviour of visitors to services. The purpose of the Google Analytics component is to analyse the traffic on the Services. This analysis is mainly for the optimisation of the Services and in order to carry out a cost-benefit analysis of Internet advertising.

Google, through its Web Analytics service collects, among other things, data about from which services a person has come to another service (the so-called referrer). It also collects which sub-pages were visited or how often and for what duration a sub-page was viewed.

Google uses the collected data and information, among other things, to evaluate the use of the Services, to provide online reports and to provide other services concerning the use of the Services for us.

This information doesn't identify visitors or collect any personal details. We don't make any attempt to find out the identities of those accessing the Services. We won't associate any data gathered from this site with any Personal Data from any source. We'll make it clear when we collect Personal Data and will explain what we intend to use it for.

Here are the details for the operating company of the Google Analytics component:

Google Inc.

Business Address:
1600 Amphitheatre Pkwy, Mountain View, California 94043-1351, United States

Registered Address:
1600 Amphitheatre Pkwy, Mountain View, California 94043-1351, United States

Contact Information:
Website: https://www.google.com

Data Location(s):
Geographically distributed set of data centres that's designed to maintain service continuity in the event of a disaster or other incident in a single region.

Data Protection and Privacy Policy:
https://policies.google.com/privacy

For the web analytics through Google Analytics we use the application "_gat. _anonymizeIp". By means of this application the IP address of your Internet connection is abridged by Google and anonymised when accessing the Services.

Google Analytics places a cookie on your information technology system. With the setting of the cookie Google is enabled to analyse the use of the Services. With each call-up to one of the individual pages of the Services, your Internet browser will automatically submit data through the Google-Analytics component. This data is used for the purpose of online advertising and the settlement of commissions to Google. The cookie is used to store personal information, such as your access time, your location from which the access was made, and the

frequency of your visits to the Services. With each visit to the Services, such personal data, including your IP address, will be transmitted to Google. Google may pass these personal data collected through the technical procedure to third parties.

You may prevent the setting of cookies through the Services at any time by changing the settings of your web browser and thus permanently deny the setting of cookies. In addition, cookies already in use by Google Analytics may be deleted anytime via your web browser or other software programs.

In addition, you may object to, and prevent, a collection and processing of data that are generated by Google Analytics. To provide this choice on how your data is collected by Google Analytics, Google have developed the Google Analytics Opt-out Browser Add-on. The add-on communicates with the Google Analytics JavaScript (ga.js) to indicate that information about the Services visit shouldn't be sent to Google Analytics. The Google Analytics Opt-out Browser Add-on doesn't prevent information from being sent to the Services itself or to other web analytics services.

You can obtain the Google Analytics Opt-out Browser Add-on under the link https://tools.google.com/dlpage/gaoptout. The installation of the browser add-on is considered an objection by Google. If your information technology system is later deleted, formatted or newly installed, then you must reinstall the browser add-ons to disable Google Analytics. If you uninstalled or disabled the browser add-on, you'll need to reinstall or reactivate the browser add-ons to disable Google Analytics.
Google Analytics is further explained under the following
Link https://www.google.com/analytics/.

Google AdWords

We've integrated Google AdWords with the Services. Google AdWords is a service for Internet advertising that allows the advertiser to place ads in Google search engine results and the Google advertising network. In the Google Advertising Network, the ads are distributed on relevant web pages using an automatic algorithm, taking into account the previously defined keywords.

Here are the details for the operating company of the Google Analytics component:

Google Inc.

Business Address:
1600 Amphitheatre Pkwy, Mountain View, California 94043-1351, United States

Registered Address:
1600 Amphitheatre Pkwy, Mountain View, California 94043-1351, United States

Contact Information:
Website: https://www.google.com

Data Location(s):
Geographically distributed set of data centres that's designed to maintain service continuity in the event of a disaster or other incident in a single region.

Data Protection and Privacy Policy:
https://policies.google.com/privacy

The purpose of Google AdWords is the promotion of the Services by the inclusion of relevant advertising on the websites of third parties. This advertising is also included in the search engine results of the search engine Google. Google AdWords may also be used to include third-party advertising on the Services.

If you reach the Services via a Google ad, a so-called conversion cookie is filed on your information technology system through Google. A conversion cookie loses its validity after 30 days and isn't used to identify you. If the cookie hasn't expired, the conversion cookie is used to check whether certain sub-pages were called up on the Services. Through the conversion cookie, both us and Google can understand whether a person who reached an AdWords ad on the Services generated sales.

The data and information collected through the use of the conversion cookie are used by Google to create visit statistics for the Services. These visit statistics are used by us in order to determine the total number of users who have been served

through AdWords ads. We do this to ascertain the success or failure of each AdWords ad and to optimize our AdWords ads for the future. Neither our company nor other Google AdWords advertisers receive information from Google that could identify you.

The conversion cookie stores personal information, for example the Internet pages you visited. Each time we visit our Internet pages, personal data, including the IP address of the Internet access you used, are transmitted to Google. Google may pass these Personal Data collected through the technical procedure to third parties.

Further information and the applicable data protection provisions of Google may be retrieved under https://www.google.com/intl/en/policies/privacy/.

YouTube

We've integrated components of YouTube with the Services. YouTube is an Internet video portal that enables video publishers to set video clips and other users free of charge, which also provides free viewing, review and commenting on them.

Here are the details for the operating company of the Google Analytics component:

YouTube, LLC which is a subsidiary of Google Inc. (1600 Amphitheatre Pkwy, Mountain View, CA 94043-1351, UNITED STATES)

Business Address:
901 Cherry Ave., San Bruno, California 94066, United States

Registered Address:
901 Cherry Ave., San Bruno, California 94066, United States

Contact Information:
Website: https://www.youtube.com

Data Location(s):
Geographically distributed set of data centres that's designed to maintain service continuity in the event of a disaster or other incident in a single region.

Data Protection and Privacy Policy:
https://policies.google.com/privacy

With each call-up to one of the individual pages of the Services, your Internet browser is automatically prompted to download a display of the corresponding YouTube component of YouTube. Further information about YouTube may be obtained under https://www.youtube.com/yt/about/en/. In course of this technical procedure, YouTube and Google gain knowledge of what specific sub-page of the Services you accessed.
If you're logged in on YouTube, YouTube recognises with each call-up to a sub-page that contains a YouTube video, which specific sub-page of the Services you accessed. This information is collected by YouTube and Google and assigned to your YouTube account.

YouTube and Google will receive information through the YouTube component that you accessed on the Services. If you are logged in on YouTube at the time you accessed the Services; this occurs regardless of whether you click on a YouTube video or not. If such a transmission of this information to YouTube and Google isn't desirable for you, you can log off from your own YouTube account before a call-up to the Services is made.

YouTube's data protection provisions, provide information about the collection, processing and use of Personal Data by YouTube and Google. These provisions are available at https://www.google.com/intl/en/policies/privacy/.

Facebook

We've integrated components of Facebook with the Services.

Here are the details for the operating company of the Facebook component:

Facebook

Business Address:
1 Hacker Way, Menlo Park, California 94025, United States

Registered Address:
1 Hacker Way, Menlo Park, California 94025, United States

Contact Information:
Website: https://www.facebook.com/

Data Location(s):
Prineville,

Forest City,

Luleå,

Altoona,

Fort Worth,

Clonee,

Los Lunas,

Odense,

Papillion,

New Albany,

Henrico,

Newton

Data Protection and Privacy Policy:
https://www.facebook.com/privacy/explanation

Instagram

We've integrated components of Instagram with the Services.

Here are the details for the operating company of the Instagram component:

Instagram

Business Address:
1 Hacker Way, Menlo Park, California 94025, United States

Registered Address:
1 Hacker Way, Menlo Park, California 94025, United States

Contact Information:
Website: https://www.instagram.com/

Data Location(s):
Prineville,

Forest City,

Luleå,

Altoona,

Fort Worth,

Clonee,

Los Lunas,

Odense,

Papillion,

New Albany,

Henrico,

Newton

Data Protection and Privacy Policy:
https://www.instagram.com/legal/privacy/

Twitter

We've integrated components of Twitter with the Services.

Here are the details for the operating company of the Twitter component:

Twitter

Business Address:
1355 Market St #900, San Francisco, California 94103, United States

Registered Address:

1355 Market St #900, San Francisco, California 94103, United States

Contact Information:
Website: http://twitter.com/

Data Location(s):
Geographically distributed set of data centres that's designed to maintain service continuity in the event of a disaster or other incident in a single region.

Data Protection and Privacy Policy:
https://twitter.com/privacy

Google+

We've integrated components of Google+ with the Services.

Here are the details for the operating company of the Google+ component:

Google+

Business Address:
1600 Amphitheatre Pkwy, Mountain View, California 94043-1351, United States

Registered Address:
1600 Amphitheatre Pkwy, Mountain View, California 94043-1351, United States

Contact Information:

Website: https://www.google.com

Data Location(s):
Geographically distributed set of data centres that's designed to maintain service continuity in the event of a disaster or other incident in a single region.

Data Protection and Privacy Policy:
https://policies.google.com/privacy

LinkedIn

We've integrated components of LinkedIn with the Services.

Here are the details for the operating company of the LinkedIn component:

LinkedIn

Business Address:
1000 W Maude Ave, Sunnyvale, CA 94085, United States

Registered Address:
1000 W Maude Ave, Sunnyvale, CA 94085, United States

Contact Information:
Website: https://linkedin.com

Data Location(s):
Geographically distributed set of data centres that's designed to maintain service continuity in the event of a disaster or other incident in a single region.

Data Protection and Privacy Policy:
https://www.linkedin.com/legal/privacy-policy

AddThis

We've integrated components of AddThis with the Services.

Here are the details for the operating company of the AddThis component:

AddThis

Business Address:
1595 Spring Hill Rd, Suite 300, Vienna, VA 22182

Registered Address:
1595 Spring Hill Rd, Suite 300, Vienna, VA 22182

Contact Information:
Website: https://www.addthis.com

Data Location(s):
Geographically distributed set of data centres that's designed to maintain service continuity in the event of a disaster or other incident in a single region.

Data Protection and Privacy Policy:
http://www.addthis.com/privacy

PayPal

We've integrated components of PayPal with the Services.

Here are the details for the operating company of the PayPal component:

PayPal

Business Address:
2211 North First Street San Jose, California 95131

Registered Address:
2211 North First Street San Jose, California 95131

Contact Information:
Website: https://ww.paypal.com

Data Location(s):
Geographically distributed set of data centres that's designed to maintain service continuity in the event of a disaster or other incident in a single region.

Data Protection and Privacy Policy:
https://www.paypal.com/en/webapps/mpp/ua/privacy-full

Mailchimp

We've integrated components of Mailchimp with the Services.

Here are the details for the operating company of the Mailchimp component:

Mailchimp

Business Address:
Ponce City Market, Atlanta, Georgia

Registered Address:
Ponce City Market, Atlanta, Georgia

Contact Information:
Website: https://mailchimp.com

Data Location(s):
Geographically distributed set of data centres that's designed to maintain service continuity in the event of a disaster or other incident in a single region.

Data Protection and Privacy Policy:
https://mailchimp.com/legal/privacy

14. Transferring your data

Your Personal Data may be transferred to Third-Party Data Processors across international borders. It may also be transferred to countries that have different levels of data protection laws to the country from where you submitted your Personal Data.

Countries recognised as having an adequate level of legal protection for the rights and freedoms of Data Subjects in relation to the Processing of their Personal Data include Andorra, Argentina, Austria, Belgium, Bulgaria, Canada (commercial organisations), Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Faeroe Islands, Finland, France, Germany, Greece, Guernsey, Hungary, Iceland, Ireland, Isle of Man, Israel, Italy, Jersey, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, New Zealand, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, United Kingdom, Uruguay and United States (Privacy Shield certified organisations).

The following are a list of transfer mechanisms that can provide adequate protection when transfers are made to countries lacking an adequate level of legal protection:

- Model Clauses,
- Binding Corporate Rules,
- Codes of Conduct,
- Certification Mechanisms Derogations,
- Explicit Consent,
- Compelling Legitimate Interests,
- Important reasons of Public Interest,
- Transfers in response to a foreign legal requirement; and
- DPA approved contracts between Data Controllers and Data Processors.

All Third-Party Data Processors have been carefully selected to ensure their compliance with the GDPR and the DPA. Our collection, storage and use of your Personal Data will at all times continue to be governed by this Policy.

You acknowledge and understand that your information will be transferred, processed and stored in the country where the Services are located. This is necessary to provide the Services and perform the Terms of Service. The privacy laws may be different from those in your jurisdiction.

If data is transferred from within the EEA to a jurisdiction outside the EEA, it's done so under a Data Transfer Agreement. This agreement will contain standard data protection contract clauses. The European Commission has adopted standard data protection contract clauses (known as the Model Clauses) which provide safeguards for personal information that's transferred outside of Europe. We use Model Clauses when transferring personal data outside of Europe.

The sharing of data may involve transferring data to and from the United States. If your data is transferred to or from the United States, it will only be transferred with a Third-Party Data Processor that complies with the EU-U.S. Privacy Shield Framework. The EU-U.S. Privacy Shield Framework is set forth by the U.S. Department of Commerce regarding the collection, use, and retention of Personal Data from the European Union countries.

You can learn more about the Privacy Shield Frameworks and view certifications, by visiting the U.S. Department of Commerce's Privacy Shield website: https://www.privacyshield.gov/welcome.
A list of Privacy Shield participants is maintained by the U.S. Department of Commerce and is available at: https://www.privacyshield.gov/list.
Our website server and mobile application server may be located outside of the country from which you've accessed our website and mobile application. Our website and mobile application providers are bound by a contract that ensures your data is processed in accordance with the GDPR and the DPA.

Our IT systems may be located outside of the country from which we operate. Our IT systems provider is bound by a contract that ensures your data is processed in accordance with the GDPR and the DPA. Our IT systems provider acts only on our instructions and implements all technical measures necessary on an ongoing basis to keep your Personal Data secure.

15. Where we store your data

We may store your data on our website server, website database, mobile application server, mobile application database and IT systems. Our providers for these services are bound by a contract that ensures your data is processed in accordance with the GDPR and the DPA. Our providers for these services act only on our instructions and implement all technical measures necessary on an ongoing basis to keep your Personal Data secure.

16. How long we may store your data for

We'll retain your information, including Personal Data, only for as long as is necessary for the purposes for which is was collected, as long as it's necessary to provide the Services to you or as required by applicable laws or regulations. We may also retain your information to resolve disputes and to enforce our agreements.

Information about you that's no longer necessary and relevant to provide the Services may be anonymised and aggregated with other non-personal data. We may do this to provide insights, such as statistics of the use of the Services.

17. Controlling your data and your rights

Under the GPDR, as adopted into law of the United Kingdom in the DPA, you have the following rights:

- Right to be informed
- Right of access
- Right of rectification
- Right of erasure
- Right to restrict data processing
- Right to data portability
- Right to object
- Right to withdraw consent
- Rights related to automated decision-making and profiling

Right to be informed

You have the right to know whether your Personal Data is being processed.

If you wish to exercise this right, you may contact our DPO at any time.

Right of access

You have the right to request information about your Personal Data stored by the Data Controller for free. We can charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it's repetitive.

You can verify the details you've submitted to us by contacting our DPO. Our security procedures mean that we may request proof of identity before we reveal information, including your e-mail address and possibly your address.

Your access may be denied if making the information available would reveal Personal Data that we're legally prevented from disclosing.

Upon successful verification of your identity, you are entitled to obtain the following information about your own Personal Data:

· The purposes of the collection, Processing, use and storage of their Personal Data.

· The source(s) of the Personal Data if it was not obtained from the Data Subject.

· The categories of Personal Data stored for the Data Subject.

· The recipients or categories of recipients to whom the Personal Data has been or may be transmitted, along with the location of those recipients.

· The envisaged period of storage for the Personal Data or the rationale for determining the storage period.

· The use of any automated decision-making, including Profiling.

· The right of the Data subject to:

    - object to Processing of their Personal Data,

- lodge a complaint with the supervisory authority,
- request rectification or erasure of their Personal Data; and
- request restriction of Processing of their Personal Data.

If you wish to exercise this right, you may contact our DPO at any time. Your request will be logged as it is received, and a response will be provided within 30 days of the receipt of the written request.

Right of rectification

You have the right to rectify your incomplete or inaccurate Personal Data.

If you wish to exercise this right, you may contact our DPO at any time. Your request will be logged as it is received, and a response will be provided within 30 days of the receipt of the written request.

Right to erasure (right to be forgotten)

You have the right to erase your data without undue delay if:

· the processing of Personal Data is no longer necessary in relation to the purposes for which it was collected or processed,

· you withdraw your consent on which the processing is based and where there are no other legal grounds for the processing,

· you object to the processing and there are no overriding legitimate grounds for the processing,

· the Personal Data has been processed unlawfully,

· the Personal Data must be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject; or

· the Personal Data has been collected in relation to the offer of information society services referred to in Article 8 (1) of the GDPR.

If we've made the Personal Data public and we're obliged to erase the Personal Data, we'll take reasonable steps to inform other Data Controllers. which are processing the Personal Data.

Please note that if you've shared any information with others through social media channels, that information may remain visible, even if your account is deleted.

If you wish to exercise this right, you may contact our DPO at any time.

Right to restrict data processing

You have the right to block the processing of your data if:

· you contest the accuracy of the Personal Data, for a period enabling the Data Controller to verify the accuracy of the personal data,

· the processing is unlawful, and you oppose the erasure of the Personal Data and request instead the restriction of use,

· the Data Controller no longer needs the Personal Data for the purposes of the processing, but they're required by you,

· you object to processing pending the verification whether the legitimate grounds of the Data Controller override yours,

If you wish to exercise this right, you may contact our DPO at any time.

Right to data portability

You have the right to request that the Data Controller provides your Personal Data in a structured, commonly used and machine-readable format. You have a

further right to transmit the Personal Data to another Data Controller without hinderance.

If you wish to exercise this right, you may contact our DPO at any time.

Right to object

You have the right to object to the processing of your data. If you object we shall stop processing the Personal Data unless we can demonstrate compelling legitimate grounds.

If you wish to exercise this right, you may contact our DPO at any time.

Right to withdraw consent

You have the right to withdraw your consent to processing of your Personal Data.

We may retain data even if you withdraw your consent if we can demonstrate that we've a legal requirement to.

If you wish to exercise this right, you may contact our DPO at any time.

You can unsubscribe from marketing e-mails by clicking the "unsubscribe" link at the bottom of any e-mail. Once you do this, you'll no longer receive any e-mails from us.

Automated decision-making and profiling

You are protected from automated decision-making processes which produces legal effects or significantly affects you.

You may be subject to automated decision-making, including profiling, if:

· it's necessary for entering into, or the performance of, a contract between you and the Data Controller,

· it's authorised by law to which the Data Controller is subject to; or

· you have provided explicit consent.

If you're subject to automated decision-making, including profiling, suitable measures will be undertaken to safeguard your rights, freedoms and legitimate interests. As a minimum, we'll safeguard your right to human intervention, to express your point of view and to contest the decision.

Adjust Notification and E-mail Preferences

We offer several settings to help you manage notifications and e-mails that we may send you. You can unsubscribe from receiving e-mails from us by clicking the "unsubscribe" link at the bottom of any e-mail. Once you do this, you'll no longer receive any e-mails from us.

"Do Not Track"

Because there currently isn't an industry or legal standard for recognizing or honouring DNT signals, we don't respond to them at this time. We await the result of work by the privacy community to determine when such a response is appropriate.

18. Cookies

Cookies are small files saved to your device's hard drive. Cookies track, save and store information about your interactions and usage of the Services. Cookies can't be used to run programs or deliver viruses to your device.

Cookies allows the Services to provide you with a tailored experience and more user-friendly services. These services wouldn't be possible without the cookie setting. We also use cookies to provide us with business and marketing information and to understand how you use our Services.

'Session cookies' allow us to track your actions during a single browsing session, but they don't remain on your device afterwards.

'Persistent cookies' remain on your device between sessions. We use them to authenticate you and to remember your preferences. We can also use them to balance the load on our servers and improve your experience on our site.

Session and persistent cookies can be either first or third-party cookies. A first-party cookie is set by the website being visited; a third-party cookie is set by a different website. Both types of cookie may be used by us or our business partners.

The following first party cookies are in use on our Services:

Cookie domain: avssp.co.uk
Cookie name: Session cookie
Cookie expires after: session ends
Purpose: This is a neccessary non-persistant cookie which lasts the duration of the website session.

The following third-party cookies are in use on our Services:

Cookie domain: avssp.co.uk
Cookie name: _ga
Cookie expires after: 2 years
Purpose: This cookie is used to collect information about how visitors use our websites. It is used to compile reports and to help us improve our sites. The cookie collects information in an anonymous form.

Cookie domain: avssp.co.uk
Cookie name: _gid
Cookie expires after: 24 hours
Purpose: This cookie is used to collect information about how visitors use our

websites. It is used to compile reports and to help us improve our sites. The cookie collects information in an anonymous form.

Cookie domain: avssp.co.uk
Cookie name: _gat
Cookie expires after: 24 hours
Purpose: This cookie is used to collect information about how visitors use our websites. It is used to compile reports and to help us improve our sites. The cookie collects information in an anonymous form.

Cookie domain: avssp.co.uk
Cookie name: _gat_gtag_[id]
Cookie expires after: session ends
Purpose: This cookie is used to collect information about how visitors use our websites. It is used to compile reports and to help us improve our sites. The cookie collects information in an anonymous form.

Cookie domain: avssp.co.uk
Cookie name: _atuvc
Cookie expires after: 1 year
Purpose: This cookie is used to control the share buttons on our website.

Cookie domain: avssp.co.uk
Cookie name: _atuvs
Cookie expires after: 1 year
Purpose: This cookie is used to control the share buttons on our website.

Information obtained through cookies won't be disclosed to any Third-Party except for Third-Party Data Processors required to analyse the data. We won't sell or rent your information obtained through cookies and it won't be used for unsolicited communications.

Web browsers allow you to exercise some control of cookies through the browser settings. Most browsers enable you to block cookies or to block cookies from particular websites. Browsers can also help you to delete cookies when you close your browser. You should note however, that you may not have access to all the features of the website if you do so. Remember that if you use different computers in different locations you'll need to ensure that cookie preferences are set for each browser.

For further information about Cookies, please visit www.allaboutcookies.org.

19. Privacy Notices

Each website included in the Services will include an online 'Privacy Notice' and an online 'Cookie Notice' fulfilling the requirements of applicable law. These notices may be presented as a single notice.

20. Security

We have a number of security measures, in line with the GDPR and the DPA, in place designed to prevent data loss, preserve data integrity and regulate access to your data.

These are summarised below:

- Prevent unauthorised persons from gaining access to data processing systems in which Personal Data are processed.

- Prevent persons entitled to use a data processing system from accessing Personal Data beyond their needs and authorisations.

- Ensure that Personal Data in the course of electronic transmission during transport cannot be read, copied, modified or removed without authorisation.

- Ensure that access logs are in place to establish whether, and by whom, the Personal Data was entered into, modified on or removed from a data processing system.

- Ensure that in the case where processing is carried out by a Data Processor, the data can be processed only in accordance with the instructions of the Data Controller.

- Ensure that Personal Data is protected against undesired destruction or loss.

- Ensure that Personal Data collected for different purposes can and is processed separately.

- Ensure that Personal Data is not kept longer than necessary.

Only authorised Employees, and authorised employees of our Third-Party Data Processors have access to your Personal Data and they're required to adhere to our Data Protection and Privacy Policies and comply with the GDPR and the DPA.

All Third-Party Data Processors have been carefully selected to ensure their compliance with the GDPR and the DPA and to ensure their commitment to security. Contracts are also in place with Third-Party Data Processors to ensure that the level of security required is in place. These also ensure that your Personal Data is processed only as we instruct.

We take several measures to safeguard the collection, transmission and storage of the data we collect. Personal Data is stored using modern software that's kept up-to-date. Although we strive to employ reasonable protections for your information, we do not guarantee or warrant the security of the information you share with us. We're not responsible for the theft, destruction, loss or inadvertent disclosure of your information or content. No system is 100% secure. The Services use industry standard Secure Sockets Layer (SSL) technology to allow for the encryption of personal information and credit card numbers. We use secure servers protect this information using advanced firewall technology.

To help ensure that these measures are effective, you should be aware of the security features available to you through your browser. You should use a security-enabled browser to submit your credit card information and other personal information at the Services. Please note that if you don't use an SSL-capable browser, you're at risk for having data intercepted.

Most browsers have the ability to notify you if you:

· change between secure and insecure communications,

· receive invalid services identification information for the Services you're communicating with; or

· send information over an unsecured connection.

We recommend that you enable these browser functions to help ensure that your communications are secure. You can monitor the URL of the services you're visiting, by checking for secure URLs beginning with https:// rather than http://. You can also look for the security symbol of your browser to help identify when you're communicating with a secure server. You can also view the details of the

security certificate of the services to which you're connected. Please check the validity of any Services you connect to using secure communications.

While we continue to work hard to protect your personal information, no data transmission over the Internet can be guaranteed to be absolutely secure. We can't ensure or warrant the security of any information you transmit to us. Transmitting personal information is done at your own risk.

If we give you a password or any other security information, you must keep it confidential and not share it. Although we try to provide protection, we can't guarantee complete security for your data. You take the risk that any sending of the data turns out to be not secure despite our efforts.

If your Personal Data is destroyed, it will be done safely, and in accordance with best practice at the time of destruction. We'll make reasonable efforts to ensure that destroyed data is irrecoverable.

21. Breaches

A breach of security may lead to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. In the event of a breach we shall promptly assess the risk to people's rights and freedoms. If appropriate, we will also report this breach to the ICO.

If you suspect that a Personal Data Breach has occurred, you must immediately notify our DPO providing a description of what occurred. Our DPO will investigate all reported incidents to confirm whether or not a Personal Data Breach has occurred. If a Personal Data Breach is confirmed, our DPO will follow the relevant authorised procedure based on the criticality and severity.

22. Off-Boarding staff

A range of methods are used to ensure any personnel leaving the organisation do not continue to have access to sensitive or personal data. These include but are not limited to:

- Immediately disabling access to email
- Removing all rights and access to all applications which may hold data
- Disabling company owned mobile phone or other electronic devices

- Deleting and wiping company personal data on any employee owned mobile phone or electronic device
- Deleting data which may have been used by the departing employee

23. Email retention policy

To aim to ensure personal data is not retained within email for an undue length of time or for undue reason all email records will be wiped after 6 years.

24. Employee training

All of our Employees who have access to any kind of Personal Data will have their obligations outlined during their induction procedures. These obligations are also included in our Company Handbook and Employees must accept these along with our other policies. In addition, we will provide regular Data Protection and Privacy training and procedural guidance for our Employees.

The training and procedural guidance will consist of, at a minimum, the following elements:

· The Data Protection Principles.

· The duty to use and permit the use of Personal Data only by authorised persons and for authorised purposes.

· The need for, and proper use of, the forms and procedures adopted to implement this policy.

· The correct use of entry control.

· The correct use of passwords, security tokens and other access mechanisms.

· The importance of limiting access to Personal Data, such as by using password protected screen savers and logging out correctly.

· Securely storing manual files, print outs and electronic storage media, including our clear desk policy.

· The need to obtain appropriate authorisation and utilise appropriate safeguards for all transfers of Personal Data.

· Proper disposal of Personal Data by using secure shredding facilities.

· Any special risks associated with particular departmental activities or duties.

25. Links to other services

While using the Services, you can follow links to other services that aren't under our control. Our terms and conditions and our policies won't apply to other services that you get to via a link. Also, we're not responsible for the content or privacy policy of these other services.

26. Data Protection and Privacy by Design

We identify all Data Protection and Privacy requirements when designing new systems or processes. We also identify requirements when reviewing or expanding existing systems or processes. To facilitate this, each of them must go through an approval process before continuing.

We'll ensure that a Data Protection Impact Assessment (DPIA) is conducted for all new systems or processes. We'll also do this for revised systems and processes. The findings of any DPIA will be submitted to our board / directors for review and approval.

27. Changes

We may change this Policy and if we do, we'll post them on our website. We may also e-mail or message users, newsletter subscribers and customers about the changes.

You can request previous versions of this Policy by contacting our DPO at any time.

If you object to any of the changes to this Policy, you should stop using the Services. and delete your account.

28. Complaints

You have the right to lodge a complaint with a supervisory authority. You may wish to do this if you consider that the processing of Personal Data infringes the GDPR or the DPA.

In the first instance, you should put forward the matter in writing to our DPO. Our DPO will then carry out an investigation of the complaint. Our DPO will inform you of the progress and the outcome of the complaint within a reasonable period. If the issue cannot be resolved through consultation between you and our DPO, then you may seek redress. At your option, this redress may be through:

- mediation,
- binding arbitration,
- litigation; or
- via complaint to the supervisory authority within the applicable jurisdiction.

The Information Commissioner's Office (ICO) is the supervisory authority for the UK. To make a complaint to the ICO, you can visit https://ico.org.uk/concerns/. You can also call the ICO's helpline on 0303 123 1113.

29. Dispute Resolution

You agree to the dispute resolution terms included in our Terms and Conditions. You can find our Terms and Conditions by visiting https://www.avssp.co.uk/terms.

30. Further Information

Contact our DPO for further information regarding the data we collect and how we use it.