Schedule 20 (Processing Data)

1. **Status of the Controller**

1.1 The Parties acknowledge that for the purposes of the Data Protection Legislation, the nature of the activity carried out by each of them in relation to their respective obligations under a Contract dictates the status of each party under the DPA 2018. A Party may act as:

1.1.1 "Controller" in respect of the other Party who is "Processor";

1.1.2 "Processor" in respect of the other Party who is "Controller";

1.1.3 "Joint Controller" with the other Party;

1.1.4 "Independent Controller" of the Personal Data where the other Party is also "Controller",

in respect of certain Personal Data under a Contract and shall specify in Annex 1 *(Processing Personal Data)* which scenario they think shall apply in each situation.

2. **Where one Party is Controller and the other Party its Processor**

2.1 Where a Party is a Processor, the only Processing that it is authorised to do is listed in Annex 1 *(Processing Personal Data*) by the Controller.

2.2 The Processor shall notify the Controller immediately if it considers that any of the Controller's instructions infringe the Data Protection Legislation.

2.3 The Processor shall provide all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment prior to commencing any Processing. Such assistance may, at the discretion of the Controller, include:

2.3.1 a systematic description of the envisaged Processing and the purpose of the Processing;

2.3.2 an assessment of the necessity and proportionality of the Processing in relation to the Services;

2.3.3 an assessment of the risks to the rights and freedoms of Data Subjects; and

2.3.4 the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

2.4 The Processor shall, in relation to any Personal Data Processed in connection with its obligations under the Contract:

2.4.1 Process that Personal Data only in accordance with Annex 1 *(Processing Personal Data*), unless the Processor is required to do otherwise by Law. If it is so required the Processor shall notify the Controller before Processing the Personal Data unless prohibited by Law;

2.4.2 ensure that it has in place Protective Measures, including in the case of the Supplier the measures set out in Clause 18.4 of the Core Terms, which the Controller may reasonably reject (but failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures) having taken account of the:

a) nature of the data to be protected;

b) harm that might result from a Personal Data Breach;

c) state of technological development; and

d) cost of implementing any measures;

2.4.3 ensure that:

a) the Processor Personnel do not Process Personal Data except in accordance with the Contract (and in particular Annex 1 *(Processing Personal Data*));

b) it uses all reasonable endeavours to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:

(i) are aware of and comply with the Processor's duties under this Schedule 20, Clauses 18 (Data protection), 19 (What you must keep confidential) and 20 (When you can share information);

(ii) are subject to appropriate confidentiality undertakings with the Processor or any Subprocessor;

(iii) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Controller or as otherwise permitted by the Contract; and

(iv) have undergone adequate training in the use, care, protection and handling of Personal Data;

2.4.4 not transfer Personal Data outside of the UK unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:

a) the transfer is in accordance with Article 45 of the UK GDPR (or section 73 of DPA 2018); or

b) the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with UK GDPR Article 46 or section 75 of the DPA 2018) as determined by the Controller which could include relevant parties entering into the International Data Transfer Agreement (the "**IDTA**"), or International Data Transfer Agreement Addendum to the European Commission's SCCs (the "**Addendum**"), as published by the Information Commissioner's Office from time to time, as well as any additional measures determined by the Controller;

c) the Data Subject has enforceable rights and effective legal remedies;

d) the Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Controller in meeting its obligations); and

e) the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the Processing of the Personal Data;

2.4.5 where the Personal Data is subject to EU GDPR, not transfer Personal Data outside of the EU unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:

a) the transfer is in accordance with Article 45 of the EU GDPR; or

b) the transferring Party has provided appropriate safeguards in relation to the transfer in accordance with Article 46 of the EU GDPR as determined by the non-transferring Party which could include relevant parties entering into Standard Contractual Clauses in the European Commission's decision 2021/914/EU or such updated version of such Standard Contractual Clauses as are published by the European Commission from time to time as well as any additional measures determined by the non-transferring Party;

c) the Data Subject has enforceable rights and effective legal remedies;

d) the transferring Party complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the non-transferring Party in meeting its obligations); and

e) the transferring Party complies with any reasonable instructions notified to it in advance by the non-transferring Party with respect to the processing of the Personal Data; and

2.4.6 at the written direction of the Controller, delete or return Personal Data (and any copies of it) to the Controller on termination of the Contract unless the Processor is required by Law to retain the Personal Data.

2.5 Subject to Paragraph 2.6 of this Schedule 20, the Processor shall notify the Controller immediately if in relation to it Processing Personal Data under or in connection with the Contract it:

2.5.1 receives a Data Subject Access Request (or purported Data Subject Access Request);

2.5.2 receives a request to rectify, block or erase any Personal Data;

2.5.3 receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;

2.5.4 receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data Processed under the Contract;

2.5.5 receives a request from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or

2.5.6 becomes aware of a Personal Data Breach.

2.6 The Processor's obligation to notify under Paragraph 2.5 of this Schedule 20 shall include the provision of further information to the Controller, as details become available.

2.7 Taking into account the nature of the Processing, the Processor shall provide the Controller with assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under Paragraph 2.5 of this Schedule 20 (and insofar as possible within the timescales reasonably required by the Controller) including by immediately providing:

2.7.1 the Controller with full details and copies of the complaint, communication or request;

2.7.2 such assistance as is reasonably requested by the Controller to enable it to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;

2.7.3 the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;

2.7.4 assistance as requested by the Controller following any Personal Data Breach; and/or

2.7.5 assistance as requested by the Controller with respect to any request from the Information Commissioner's Office or any other regulatory authority, or any consultation by the Controller with the Information Commissioner's Office or any other regulatory authority.

2.8 The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this Schedule 20. This requirement does not apply where the Processor employs fewer than 250 staff, unless:

2.8.1 the Controller determines that the Processing is not occasional;

2.8.2 the Controller determines the Processing includes special categories of data as referred to in Article 9(1) of the UK GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the UK GDPR; or

2.8.3 the Controller determines that the Processing is likely to result in a risk to the rights and freedoms of Data Subjects.

2.9 The Processor shall allow for audits of its Data Processing activity by the Controller or the Controller's designated auditor.

2.10 The Parties shall designate a Data Protection Officer if required by the Data Protection Legislation.

2.11 Before allowing any Subprocessor to Process any Personal Data related to the Contract, the Processor must:

2.11.1 notify the Controller in writing of the intended Subprocessor and Processing;

2.11.2 obtain the written consent of the Controller;

2.11.3 enter into a written agreement with the Subprocessor which give effect to the terms set out in this Schedule 20 such that they apply to the Subprocessor; and

2.11.4 provide the Controller with such information regarding the Subprocessor as the Controller may reasonably require.

2.12 The Processor shall remain fully liable for all acts or omissions of any of its Subprocessors.

2.13 The Buyer may, at any time on not less than 30 Working Days' notice, revise this Schedule 20 by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to the Contract).

2.14 The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Buyer may on not less than 30 Working Days' notice to the Supplier amend the Contract to ensure that it complies with any guidance issued by the Information Commissioner's Office.

3. **Where the Parties are Joint Controllers of Personal Data**

3.1 In the event that the Parties are Joint Controllers in respect of Personal Data under the Contract, the Parties shall implement Paragraphs that are necessary to comply with UK GDPR Article 26 based on the terms set out in Annex 2 to this Schedule 20 (*Processing Data*).

Independent Controllers of Personal Data

3.2 With respect to Personal Data provided by one Party to another Party for which each Party acts as Controller but which is not under the Joint Control of the Parties, each Party undertakes to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Controller.

3.3 Each Party shall Process the Personal Data in compliance with its obligations under the Data Protection Legislation and not do anything to cause the other Party to be in breach of it.

3.4 Where a Party has provided Personal Data to the other Party in accordance with Paragraph 3.2 of this Schedule 20 above, the recipient of the Personal Data will provide all such relevant documents and information relating to its data protection policies and procedures as the other Party may reasonably require.

3.5 The Parties shall be responsible for their own compliance with Articles 13 and 14 UK GDPR in respect of the Processing of Personal Data for the purposes of the Contract.

3.6 The Parties shall only provide Personal Data to each other:

3.6.1 to the extent necessary to perform their respective obligations under the Contract;

3.6.2 in compliance with the Data Protection Legislation (including by ensuring all required data privacy information has been given to affected Data Subjects to meet the requirements of Articles 13 and 14 of the UK GDPR); and

3.6.3 where it has recorded it in Annex 1 *(Processing Personal Data).*

3.7 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, each Party shall, with respect to its Processing of Personal Data as Independent Controller, implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1)(a), (b), (c) and (d) of the UK GDPR, and the measures shall, at a minimum, comply with the requirements of the Data Protection Legislation, including Article 32 of the UK GDPR.

3.8 A Party Processing Personal Data for the purposes of the Contract shall maintain a record of its Processing activities in accordance with Article 30 UK GDPR and shall make the record available to the other Party upon reasonable request.

3.9 Where a Party receives a request by any Data Subject to exercise any of their rights under the Data Protection Legislation in relation to the Personal Data provided to it by the other Party pursuant to the Contract **("Request Recipient")**:

3.9.1 the other Party shall provide any information and/or assistance as reasonably requested by the Request Recipient to help it respond to the request or correspondence, at the cost of the Request Recipient; or

3.9.2 where the request or correspondence is directed to the other Party and/or relates to that other Party's Processing of the Personal Data, the Request Recipient will:

a) promptly, and in any event within five (5) Working Days of receipt of the request or correspondence, inform the other Party that it has received the same and shall forward such request or correspondence to the other Party; and

b) provide any information and/or assistance as reasonably requested by the other Party to help it respond to the request or correspondence in the timeframes specified by Data Protection Legislation.

3.10 Each Party shall promptly notify the other Party upon it becoming aware of any Personal Data Breach relating to Personal Data provided by the other Party pursuant to the Contract and shall:

3.10.1 do all such things as reasonably necessary to assist the other Party in mitigating the effects of the Personal Data Breach;

3.10.2 implement any measures necessary to restore the security of any compromised Personal Data;

3.10.3 work with the other Party to make any required notifications to the Information Commissioner's Office or any other regulatory authority and affected Data Subjects in accordance with the Data Protection Legislation (including the timeframes set out therein); and

3.10.4 not do anything which may damage the reputation of the other Party or that Party's relationship with the relevant Data Subjects, save as required by Law.

3.11 Personal Data provided by one Party to the other Party may be used exclusively to exercise rights and obligations under the Contract as specified in Annex 1 *(Processing Personal Data).*

3.12 Personal Data shall not be retained or processed for longer than is necessary to perform each Party's respective obligations under the Contract which is specified in Annex 1 *(Processing Personal Data)*.

3.13 Notwithstanding the general application of Paragraphs 2.1 to 2.14 of this Schedule 20 to Personal Data, where the Supplier is required to exercise its regulatory and/or legal obligations in respect of Personal Data, it shall act as an Independent Controller of Personal Data in accordance with Paragraphs 3.2 to 3.12 of this Schedule 20.

Annex 1 - Processing Personal Data

1. This Annex shall be completed by the Controller, who may take account of the view of the Processor, however the final decision as to the content of this Annex shall be with the Buyer at its absolute discretion.

   1.1 The contact details of the Buyer's Data Protection Officer are:

   XXX Redacted under FOIA Section No: 40 – Personal Information

   email: XXX Redacted under FOIA Section No: 40 – Personal Information

   The contact details of the Supplier's Data Protection Officer are:

   XXX Redacted under FOIA Section No: 40 – Personal Information

   Email: XXX Redacted under FOIA Section No: 40 – Personal Information

   1.2 The Processor shall comply with any further written instructions with respect to Processing by the Controller.

   1.3 Any such further instructions shall be incorporated into this Annex.

Description	Details
Identity of Controller for each Category of Personal Data	**The Buyer is Controller and the Supplier is Processor** The Parties acknowledge that in accordance with Paragraph 2 and for the purposes of the Data Protection Legislation, the Buyer is the Controller and the Supplier is the Processor of the Personal Data collected through the provision of goods and services under DVSA contract K280022019 PPE & Corporate Clothing.
Duration of the Processing	DVSA requires that all personal data should be retained by the Supplier no longer than six full fiscal years plus after one year after the expiry date of the contract; this is to enable full reporting of P11d liabilities, should this be a future requirement.
Nature and purposes of the Processing	We need the personal data we collect from you to contact you in order to arrange delivery or collection of a clothing order.
Type of Personal Data	Staff Name Telephone Number Home Address Email Address

Categories of Data Subject	DVSA Staff (including volunteers, agents, and temporary workers)
Plan for return and destruction of the data once the Processing is complete UNLESS requirement under law to preserve that type of data	Arrangements will be agreed between DVSA and the Supplier prior to contract expiry for the full transfer of DVSA data held by the Supplier at the point of contract expiry. This will be contained within the Exit Management Plan (see K280022019 Schedule 30 (Exit Management))
Locations at which the Supplier and/or its Sub-contractors process Personal Data under this Contract	Burlington Uniforms Ltd 76 Lockfield Avenue Enfield Middx EN3 7PX Burlington Uniforms Ltd Unit 2 , Llewellyn's Quay The Docks Port Talbot SA13 1RF
Protective Measures that the Supplier and, where applicable, its Sub-contractors have implemented to protect Personal Data processed under this Contract Agreement against a breach of security (insofar as that breach of security relates to data) or a Personal Data Breach	**POL 016** **Burlington Uniforms Limited** **Data Breach Policy** **Introduction** Burlington Uniforms acknowledges that the UK General Data Protection Regulation imposes on it an obligation to report certain types of personal data breach to the Information Commissioner. This must happen within 72 hours of becoming aware of the breach, where feasible. • If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, those individuals must be informed without delay. • The company seeks to ensure that it has robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not the company is required to notify the relevant supervisory authority and the affected individuals. • The company will keep a record of any personal data breaches, regardless of whether it required to notify. **Data Protection Team**

The Data Protection Team will be responsible for the formulation, implementation and review of this policy. The Team will be constituted by:

Adrian Hewitt (Managing Director and Confidentiality Officer)
Tristan Weedon (General Manager)
Peter Blunden (Systems and Quality Manager)

Definitions
Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.
Notifiable Breach (Information Commissioner) means a breach following which it is likely that there is a risk to individuals' rights and freedoms.
Notifiable Breach (Individual) is a breach which is likely to result in a high risk to the rights and freedoms of individuals.
Rights and freedoms of individuals includes the freedom of association, employment, movement, person, speech, work or professional practice or any other activity not restricted by lawful authority; right to integrity of the person including mental and emotional well-being; rights in or over real or personal property including information and intellectual property; rights to confidentiality, privacy, reputation and standing and right not to suffer discrimination.

Assessment of Risk
Every risk identified is assessed and scored for both Impact and Likelihood on a Low/Medium/High scale. The following definitions and scoring criteria used:

Impact is the measure for any particular uncertainty of the effect on the rights and freedoms of individuals.

Low	Effect would be insignificant or manageable with available reso
Medium	Would cause difficulties requiring significant or diversion of (or resources by individuals affected by the breach.
High	Effect would be serious enough seriously to undermine, cause damage or put to expense the individuals whose data has bee by a data breach and could require intervention or assistance b parties to mitigate loss or prevent further loss or damage.

Likelihood is the expected probability of the occurrence of the uncertain event assessed after taking into account any mitigating factors and the active management or operational actions in place to reduce the likelihood.

Low	Extremely unlikely
Medium	Possible but not very likely

High	Probable

The risk rating is generated with reference to the combination of the two scores as Low, Medium or High according to the risk order matrix set out in Appendix 1 of POL 013 (Risk).

Occurrence of Breach
Any employee who discovers a data breach or has a data breach reported to him or her will immediately inform the Confidentiality Officer or other member of The Data Protection Team.

The Data Protection Team will immediately try to assess what is the cause and nature of the breach, whether it is deliberate or accidental, immediate corrective action, corrective action to prevent recurrence and whether the breach is reportable. If the Team is unable to assess all or any of these factors it will immediately call in the Company's IT support company, Replentec, who provide 365 days a year cover and have remote access to the company's IT system.

The Data Protection Team will record: a summary of the event and the circumstances (time, date, who discovered/reported, incident, responsibility), the data impacted, the individuals or group(s) of individuals affected, the risk of harm, the likely consequences of the breach, corrective and preventive action and the likelihood of recurrence.

If the Data Protection Team considers that the risk is not reportable it will record the reasons for so deciding. If in doubt the Team will report. If it is reportable it will complete FOR 085. Copies will be sent to the Information Commissioner and (if required) to the individuals affected or likely to be affected. The Confidentiality Officer will keep an office copy of the completed form.

Reports must be transmitted within 72 hours. If this is not possible the reason must be provided to the Information Commissioner and the individuals to whom reports are being sent.

Related Documents
Burlington Uniforms maintains a Policy on Security and Confidentiality (POL 007). Amongst other matters this sets out basic protocols to be followed on a day-to-day basis to prevent accidental loss or deliberate misuse of data. It also sets out the System Security Measures that are in place to prevent the leaking of data to unauthorised sources and the protection of our systems from cyber attacks.

General Matters

	This policy is a document within our Integrated Management System. It will be reviewed annually and following review circulated to all staff to be read and signed as read. Signed: XXX Redacted under FOIA Section No: 40 – Personal Information Date: 21st July 2023 Review Date: 19th July 2024