Security And Confidentiality Policy

Burlington Uniforms is a responsible member of the business community. We acknowledge that we have responsibility to seek to ensure the security of individuals working on our premises or who are or might be affected by our operations, the security of real or personal property whether belonging to the company or to any other legal person and the security of information including personal data.

This document sets out the parameters for the achievement of the highest level of security, and the procedures that will be followed to achieve these levels. This policy covers security of persons and property, goods in transit, intellectual property, information and data. It also covers the rights that individuals have under the UK General Data Protection Regulation (UK GDPR).

Burlington Uniforms' policies and procedures that touch and concern security and confidentiality reflect the provisions of UK GDPR and the Data Protection Act 2018. Although not all the rights created or enjoyed under UK GDPR are property rights they are nevertheless rights to be protected so it is right to consider them under the ambit of security. The Data Protection (Charges and Information) 2018 Regulations set out the regime for notification and payment of fees.

Responsibility

Senior management is responsible for the formulation, implementation and review of the company's policies on Security and Confidentiality. The Managing Director is ultimately responsible for ensuring that this policy and its implementation is compliant with UK GDPR and any U.K. primary or secondary legislation. This policy and related procedures are documented within the company's Integrated Management System, which has ISO 9001:2015 (quality) and ISO 14001:2015 (environmental) certification. The policy will be subject to audit and review and will be re-issued annually.

Protection of Persons and Property

Burlington Uniforms will maintain measures to ensure the security of its premises and persons on the premises (see POL 012).

All premises are alarmed with a connection to a central monitoring station. The monitoring station will be alerted in the event of burglary or attempted burglary, fire or damage to premises.

Premises are protected by a system of secondary grilles and shutters that are activated before premises are left unattended at night, weekends, and holiday periods. In the event of a fire, burglary, attempted burglary or damage to property, senior management are contacted by the monitoring station. Senior management have access to CCTV images on screen and on their mobile telephones.

During working hours there is access to premises only by entry-phone so that unauthorised access is prevented.

Our Health and Safety Policy contains instructions for dealing with bomb alerts, fire and similar emergencies that present a risk or risks to life and limb (see POL 008b).

No employee is to enter company premises alone outside business hours, at weekends or holiday periods without informing the Managing Director or General Manager. They are to report by telephone when they leave and are outside the premises so that management may know that they are safe (see POL 008b).

As well as protecting persons and real property the protocols described are intended to protect plant, machinery, computer equipment and stock whether it is Burlington Uniforms' stock or customer dedicated stock. Burlington Uniforms also has in mind protection of branding and branded stock in order to prevent theft of such stock and subsequent impersonation of clients' staff.

Electronic copies of branding are accessed through our password protected IT System. Paper copies are locked away.

Goods in Transit

A detailed record is kept of goods leaving our premises. Carriers operate a track and trace system and consignments require a signature on delivery. With these checks in place the recipient will be able to see the number and type of garments despatched from our premises and therefore the number and type of garments they should be receiving: shortages can be readily identified. Protection of branding is also a consideration as is protection of information and data.

Burlington Uniforms has a supplier selection procedure within its Integrated Management System which includes consideration of security and reliability of delivery methods employed.

Security of Suppliers' Premises

Burlington Uniforms is aware of the adverse impact on the company and/or its customers if there is a fire or security breach at a supplier's premises. This could impact upon supply, integrity of intellectual property and asset value where there was loss of damage to stock title to which had already passed to us or to a customer. Consequently our supplier assessment includes assessment of the risk of lack of or compromised security of suppliers' premises and the risk of insufficient measures in place to guard against loss of information, data or intellectual property.

Deliveries and Visits to High Security Locations

Deliveries to high security locations will be undertaken by our couriers and/or logistics providers. They have rigorous procedures for vetting staff prior to and during employment. They also treat data as an asset to be protected at all times.

Burlington Uniforms staff from time to time visit high security locations for review meetings and carrying out measuring and sizing exercises. They are instructed in the importance of following directions given to them and remaining within permitted areas. They are also trained in the importance of maintaining strict confidence in respect of any information disclosed to them or observed by them in relation to client personnel and premises.

Where considered necessary we will carry out risk assessments prior to commissioning a delivery or visit to customer premises. Such assessments will cover risk to persons, property and goods in transit during the course of delivery. They will also cover such risks that may be inherent as a result of operations carried out on customer's premises by our staff or agents.

Data, Information and Intellectual Property

We treat data as an asset that must be protected against loss and unauthorised access. We employ information security techniques to protect information from unauthorised access by users inside and outside the company.

Data Held About Individuals

Burlington Uniforms is aware of the following definitions and has had them in mind when forming procedures and policies and implementing data protection measures.

Definitions

“Personal data” means any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

Personal identifiers that can constitute personal data include name, identification number, location data or online identifier.

Personal data includes automated personal data and manual filing systems where personal data is accessible according to specific criteria.

“Data controller” means a person who (either alone or jointly or in common with other persons).

“Data subject” means an individual who is the subject of personal data.

Registration

The Company is registered with the Information Commissioner’s Office. The Data Protection (Charges and Information) Regulations 2018 sets out the regime for notification and payment of fees.

Purposes for which Data is held

Individuals about whom we will hold data:

Wearers
Supervisors/Managers/Procurement or Ordering Officers

Information that we hold or might hold about individuals Wearers:

- Name
- Job title
- Staff number
- Name of employer
- Type of work
- Length of service
- Work address
- Work email address
- Work telephone number(s)
- Work fax
- Mobile number
- Home address
- Home email
- Name of supervisor/manager
- Garments ordered
- Size
- Value of spend
- Feedback and comment
- Burlington Uniforms’ notes on possibility of adding value or improvement
- Medical conditions/disabilities.

Supervisors/Managers/Procurement or Ordering Officers

- Name
- Job title
- Name of employer
- Type of work
- Length of service
- Work address
- Work email address
- Work telephone number(s)
- Work fax
- Mobile number
- Names of those they manage/supervise
- Garments ordered or authorised
- Value of spend authorised
- Feedback and comment.

Burlington Uniforms' notes on possibility of adding value or improvement.

Partners in firms ordering from us

- Name
- Name of businesses
- Names of partners
- Nature of business
- Address of business
- Telephone number(s)
- Fax numbers
- Email addresses
- Mobile number
- Names of employees
- Garments ordered for or by employees
- Spend of business
- Credit rating of business
- Credit card details
- Bank details
- Other wearer information if partner(s) are wearers.

Sole traders ordering from us

- Name
- Name of businesses
- Nature of business
- Address of business
- Telephone number(s)
- Fax numbers
- Email addresses
- Mobile number
- Names of employees
- Garments ordered for or by employees
- Spend of business
- Credit rating of business
- Credit card details
- Bank details
- Other wearer information if proprietor is wearer.

Individuals ordering from us in private capacity

- Name
- Type of work
- Work address
- Work email address
- Work telephone number(s)
- Work fax
- Mobile number
- Home address
- Home email
- Garments ordered
- Size
- Value of spend
- Credit rating
- Medical conditions/disabilities
- Credit card details
- Bank details.

Suppliers/service providers (Partnerships, sole traders, contacts within businesses)

Partners and Proprietors

- Name
- Name of businesses
- Names of partners
- Nature of business
- Address of business
- Telephone number(s)
- Fax numbers
- Email addresses
- Mobile number
- Names of employees
- Spend with business
- Goods or services ordered
- Credit rating of business
- Bank details.

Contacts within businesses

- Name
- Job title
- Name of employer
- Type of work
- Length of service
- Work address
- Work email address
- Work telephone number(s)
- Work fax
- Mobile number.

Consultants/Professional Advisers

Partners and Proprietors

- Name
- Name of businesses
- Names of partners
- Nature of business
- Address of business
- Telephone number(s)
- Fax numbers
- Email addresses
- Mobile number
- Names of employees
- Spend with business
- Goods or services ordered
- Credit rating of business
- Bank details.

Contacts within businesses (including limited companies and limited liability partnerships)

- Name
- Job title
- Name of employer
- Type of work
- Length of service
- Work address
- Work email address
- Work telephone number(s)
- Work fax
- Mobile number.

Employees

- Name
- Address
- Telephone number
- Email addresses
- Mobile number
- Job title
- Length of services
- Date of birth (When supplied)
- Contract of employment
- Salary details
- PAYE details
- Sickness and sick pay
- Attendance records
- Training and appraisal records
- Expressions of opinion by them or about them
- Pension matters
- Medical conditions.

Sources of Information

Wearers

- Sales orders (email, fax, web orders, wardrobe management system)
- Direct oral or email communication
- Contract documentation.

Supervisors/Managers/Procurement or Ordering Officers

- Sales orders (email, fax, web orders, wardrobe management system)
- Direct oral or email communication
- Tender, PQQ documents, etc.
- Contract/account opening documentation.

Partners in firms ordering from us

- Sales orders (email, fax, web orders, wardrobe management system)
- Direct oral or email communication
- Tender, PQQ documents etc.
- Research of information in the public domain (e.g. professional bodies, websites, credit reference agencies)
- Contract/account opening documentation.

Sole traders ordering from us

- Sales orders (email, fax, web orders, wardrobe management system)
- Direct oral or email communication
- Tender, PQQ documents etc.
- Research of information in the public domain (e.g. professional bodies, websites, credit reference agencies)
- Contract/account opening documentation.

Individuals Ordering from us in private capacity

- Sales orders (email, fax, web orders, wardrobe management system)
- Direct oral or email communication
- Research of information in the public domain (e.g. professional bodies, websites, credit reference agencies)
- Contract/account opening documentation.

Suppliers/service providers (Partnerships, sole traders, contacts within businesses)

Partners and Proprietors

- Direct oral or email communication
- Research of information in the public domain (e.g. professional bodies, websites, credit reference agencies)
- Contract/account opening documentation.

Contacts within businesses

- Direct oral or email communication
- Research of information in the public domain (e.g. professional bodies, websites, credit reference agencies)
- Contract/account opening documentation.

Consultants/Professional Advisers

- Direct oral or email communication
- Research of information in the public domain (e.g. professional bodies, websites, credit reference agencies)
- Contract/account opening documentation.

Partners and Proprietors

- Direct oral or email communication
- Research of information in the public domain (e.g. professional bodies, websites, credit reference agencies)
- Contract/account opening documentation.

Contacts within businesses

- Direct oral or email communication
- Research of information in the public domain (e.g. professional bodies, websites, credit reference agencies)
- Contract/account opening documentation.

Employees

- Direct oral, written or email communication
- CVs
- Previous employers
- Management
- Medical practitioners.

Rules For The Holding and Processing Of Data On Individuals by the Company

Data on individuals will be held and processed in accordance with Article 5 of the UK GDPR and will therefore be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are accurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals; and

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

Pursuant to Article 5(2) of the UK GDPR, Burlington Uniforms acknowledges that as a data controller it shall be responsible for, and be able to demonstrate, compliance with the principles.

Lawful basis for Processing and Use of Data

Customers and Wearers

Burlington Uniforms will hold and process the information it holds for employees of Organisations (where the contract is between Burlington Uniforms and the Organisation as opposed to between Burlington Uniforms and the Employee) for the purposes of fulfilling its obligations under its contract with the Organisation. It will also hold and process personal data for the purposes of providing management information, seeking to provide added value and best value and for identifying means of achieving continuous improvement in goods and service. Personal data will also be held and processed for the purpose of identifying and dealing with complaints and issues.

Personal data may also be used for the purposes of defending any claim brought by any person against Burlington Uniforms in contract or tort. Personal data may also be used by Burlington Uniforms for the purposes of prosecuting such a claim. It may be necessary to include personal information in pleadings or witness statements and documents containing personal information may have to be disclosed and inspected. It may be transmitted to solicitors or counsel for the purpose of obtaining advice or drafting documents for issue and service. In these circumstances Burlington Uniforms is acting as a controller in its own right and will not as a joint controller or processor on behalf of another.

In respect of the purposes set out above Burlington Uniforms has a legitimate interest in holding and processing personal data as also does the Organisation and do the wearers. See Article 6(1)(f) and Recital 47 of UK GDPR.

Burlington Uniforms may from time to time be required to produce records of sales containing personal data to Her Majesty's Revenue and Customs or other government agencies. To this end data is held or processed in anticipation of or compliance with an anticipated legal obligation. See Article 6(1)(c) and Recitals 14 and 45 of UK GDPR. We may also be required or decide to provide personal information to the police or National Crime Agency. We may need to seek legal advice before so doing. In these circumstances Burlington Uniforms is again acting as a controller in its own right and will not as a joint controller or processor on behalf of another.

Where Burlington Uniforms enters into a contract with a wearer or has pre-contractual dealings with a wearer it can rely upon the lawful basis that processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract. Thus we can can rely on this lawful basis where we need to process someone's personal data to fulfil our contractual obligations to them or because they have asked us to do something before entering into a contract (e.g. provide information, illustrations or quotes). See Article 6(1)(b) and Recital 44 UK GDPR.

It will sometimes be necessary to receive, hold and process data about a wearer's medical condition or disability in order that we can cater for them in the supply of uniform. This is sensitive personal data and we will always obtain the wearer's explicit consent to hold and process the data at the time we receive the appropriate order. Where sensitive personal information is included in work instructions or orders the relevant documents will be anonymised.

Save as set out below (access to data) we will never share personal data with any third party.

Suppliers/service providers, Consultants, Professional Advisers etc. (Partnerships, sole traders, contacts within businesses)

Burlington Uniforms will hold personal information for individuals employed by businesses with whom we place business, obtain services, professional advice etc. The purpose of holding such information will be the fulfilment of our contractual obligations to the relevant organisation, achieving the aims of the contract into which we have entered and maintaining dialogue and communication with the organisation. Again, personal data may also be used for the purposes of defending any claim brought by any person against Burlington Uniforms in contract or tort. Obviously all parties will have a legitimate interest in Burlington Uniforms holding and processing this information: see Article 6(1)(f) and Recital 47 of UK GDPR.

In many instances Burlington Uniforms will have a direct contractual nexus between it and the individuals such as when dealing with partners in partnerships or sole traders. In these instances we will be able to rely on Article 6(1)(b) and Recital 44 UK GDPR (contract). Sometimes personal information will be exchanged for the purposes of inquiry before we enter into a contract.

Burlington Uniforms may from time to time be required to produce records of purchases containing personal data to Her Majesty's Revenue and Customs or other government agencies. To this end data is held or processed in anticipation of or compliance with an anticipated legal obligation. See Article 6(1)(c) and Recitals 14 and 45 of UK GDPR. It may be necessary to include personal information in pleadings or witness statements and documents containing personal information may have to be disclosed and inspected. It may be transmitted to solicitors or counsel for the purpose of obtaining advice or drafting documents for issue and service. In these circumstances Burlington Uniforms is acting as a controller in its own right and will not as a joint controller or processor on behalf of another.

Save as set out below (access to data) we will never share personal data with any third party.

Staff and Applicants for Employment

One lawful basis for holding and processing personal information about employees will be that set out in Article 6(1)(b) and referred to in Recital 44 UK GDPR that is to say the performance and monitoring of the contract of employment between the employer and employee. There may be instances where employer and employee have a legitimate interest in the company holding data where a matter is not strictly one of contract and the company will rely on Article 6(1)(f) and Recital 47 of UK GDPR.

Burlington Uniforms has an ongoing obligation to submit PAYE returns to Her Majesty's Revenue and Customs which will contain personal data about individuals and may from time to time be subject to more detailed inquiry by Her Majesty's Revenue and Customs or other government agencies. To this end data is held or processed in anticipation of or compliance with an anticipated legal obligation. See Article 6(1)(c) and Recitals 14 and 45 of UK GDPR.

Apart from the employment contract Burlington Uniforms has duties of care imposed upon it by the common law and various statutes and regulations. Under this head we will again rely upon Article 6(1)(c) and Recitals 14 and 45 of UK GDPR.

The company will rely on Article 6(1)(b) in respect of information obtained from candidates for employment including those who are unsuccessful.

Period for Retention of Data

Clients, managers, supervisors and members of wearer groups

Under this head, Burlington Uniforms will hold data about individuals for eight years following the end of the contract with the customer or eight years of being informed that an individual is no longer a member of a group of individuals about whom we hold data.

The period of eight years has been decided upon having regard to HMRC requirements to hold records for the current year and the six previous financial years.

We have also considered the ordinary time limits in contract and tort for bringing an action. These time limits are six years from the date a cause of action arises or, in the case of fatalities or personal injuries, three years. In the latter case however there is a secondary limitation period which does not begin to run until the claimant has knowledge required for bringing an action for damages in respect of the relevant damage and the right to bring such an action.

We have taken into account the need to have information available to monitor performance, seek continuous improvement and to provide management information and ad hoc reports to the customer.

Inquirers

Under this head we are thinking of circumstances where personal information is provided to us to enable us to answer pre-contract inquiries, submit tenders, quotes etc. In the circumstances that an inquiry is made but no contract results, information will be deleted six months after the last correspondence.

Suppliers/service providers, Consultants, Professional Advisers etc. (Partnerships, sole traders, contacts within businesses)

Burlington Uniforms will hold data about individuals for eight years following the end of the contract with the organisation or eight years of ascertaining that an individual is no longer a member of a group of individuals about whom we hold data.

Again we have had regard to HMRC requirements to hold records for the current year and the six previous financial years.

We have again considered the time limits in contract and tort for bringing an action as mentioned above and we have taken into account the need to have information available to monitor performance and seek continuous improvement.

Inquiries

Where we make inquiries before entering into a contract but no contract results any personal information obtained during the course of such inquiries will be deleted after six months of the last correspondence.

Employees and candidates for employment

Burlington Uniforms, applying the same considerations as under the headings above, will hold data about employees for eight years following the termination of the contract of employment.

Unsuccessful candidates

Personal information acquired from those who are unsuccessful in their application for employment will be deleted after six months of a rejection being communicated.

Marketing

Burlington Uniforms may wish to use information that it holds on individuals for the purposes of marketing. Individuals will include partnerships and sole traders and will also include individuals who are employed by companies or other bodies corporate for whom we hold contact details. We may also use information that we hold about wearers in order to hold meaningful dialogue with businesses.

Telephone Calls

We may call individuals and companies with whom we have already done business, those who have visited our website or made other inquiries (i.e. by telephone, fax, email, letter) or those whose information we have obtained through market research.

In calling such individuals we will be relying upon Article 6(1)(f) and Recital 47 of UK GDPR i.e. legitimate interest. We have a right to run a business and an interest in making and keeping it profitable, providing employment and business for our suppliers and service providers. We balance this against the possibility of causing minor inconvenience to those we contact.

We will not contact those who have registered under the Telephone Preference Scheme, the Corporate Telephone Preference Scheme or who have told us that they do not wish to be contacted. Wherever possible we will obtain actual consent to telephone contact by placing opt in statements on the website or in emails.

Letters, Circulars, Flyers etc.

The same principles and protocols as those set out above will be applied to these means of marketing, save that there is no equivalent to the Telephone Preference Scheme or Corporate Preference Telephone Scheme.

Electronic Communications (emails, texts, faxes etc.)

As well as being governed by the UK GDPR use of personal information for the purpose of marketing by means of electronic media is also affected by the Privacy and Electronic Communications (EC Directive) Regulation 2003. The effect of this is that we cannot rely on Article 6(1)(f) (legitimate) interest as the lawful basis for processing information for marketing by electronic means. We have to rely on freely given consent under Article 6(1)(a). Therefore consent to communicate in this manner will be requested when an inquirer visits our website, places an order through our website, by email or fax.

Cookies

Consent to cookies on our website will be given by visitors through clear affirmative action, such as clicking an opt-in box or choosing settings or preferences on a settings menu.

Rights of Data Subjects

Burlington Uniforms acknowledges the rights of data subjects set out in the UK GDPR, namely:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

The following rights are the most pertinent for Burlington Uniforms Limited:

Right to be informed

Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the UK GDPR.

We must provide individuals with information including: our purposes for processing their personal data, our retention periods for that personal data, and whom it will or might be shared with.

Where we obtain personal data from other sources (e.g. personal data about wearers from a supervisor), we will provide individuals with privacy information within a reasonable period of obtaining the data and no later than one month.

Right of Access

Under the UK GDPR, individuals have the right to obtain confirmation that their data is being processed; access to their personal data; other supplementary information which corresponds to information to be provided under the right to be informed and which should be contained in a privacy statement: see Article 15 UK GDPR.

Right to Erasure

Individuals have the right to have their personal data erased if the personal data is no longer necessary for the purpose for which we originally collected or processed it; we are relying on consent as the lawful basis for holding the data, and the individual withdraws their consent; we are relying on legitimate interests as our basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing; we are processing the personal data for direct marketing purposes and the individual objects to that processing; we have processed the personal data unlawfully (i.e. in breach of the lawfulness requirement of the 1st principle); we have to do it to comply with a legal obligation (e.g. a contractual provision).

The request of the data subject has to be be balanced against the data controller's own legal obligations or potential legal obligations. Having regard to the provision concerning Period for Retention of Data it is unlikely that we would agree to erase data before the period therein defined.

Security, Confidentiality and Storage of Data

Security of data is paramount. Information is stored on the company's server across a number of hard drives. It is backed up daily on a network of secondary drives. It is also backed up on portable hard drives which are removed from the premises overnight and at weekends and holidays.
E-mails are stored "in the cloud". Information obtained through on-line ordering facilities is stored on a hosting server.

Data is treated as an asset that must be protected against loss and unauthorised access. Information security techniques are employed to protect information from unauthorised access by users inside and outside the scheme. There are rigorous procedures for copying data and securely storing disks, memory sticks, paper copies, etc.

In particular personal information should:

- If in hard copy be kept in a locked filing cabinet, drawer, or safe; or
- If it is computerised, be encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up, be subject to user/share level security, virus protection, back-up systems, dedicated servers and internal procedures; and
- If redundant, should be securely cleaned from electronic storage or securely shredded.

Remote use of Data

It will sometimes be necessary for the directors, authorised employees, or properly appointed agents of or consultants to the company to hold or process information at home or other remote sites. Some such individuals have remote access to the company's system.

In cases where such off-site processing is felt to be necessary or appropriate, the agreement of the Managing Director must be obtained, and all the security guidelines given in this document must still be followed.

Where personal data is being carried off-site e.g. where sizing information is being brought back to headquarters following a measuring and sizing exercise at a client's site, a risk assessment will be carried out and suitable protocols laid down.

Data stored on portable electronic devices or removable media is the responsibility of the individual who operates the equipment. It is the responsibility of this individual to ensure that:

- consideration is given to the risks of failure to provide adequate security, which may be so high that the data should never be taken off site,
- suitable back-ups of the data exist,
- personal data is appropriately encrypted,
- personal data is not copied onto portable storage devices without first consulting the IT Director or Operations Manager, in regard to appropriate encryption and protection measures,
- electronic devices such as laptops or PDAs, and computer media (USB devices, CD-ROMs, etc.) that contain sensitive data are not left unattended when off site,
- for some information the risk of failure to provide adequate security is so great that it should never be taken or transmitted off site and top management should periodically review all personal information in order to identify any that is in this risk category.

Access to Data

Information held about individuals will only be accessed or viewed by the following persons:

- Directors, managers and other authorised employees,
- Properly appointed and authorised consultants,
- The company's accountants, solicitors, bankers or other professional advisers,
- Any court of recognised jurisdiction or any person to whom such court orders data to be disclosed,
- Such government departments and agencies to whom the Company is from time to time required to provide data,
- Our carriers (delivery details only),
- Where there is a contractual nexus with an individual with banks and clearing houses so that we can process payments.

Burlington Uniforms sees that only relevant personal information is viewed by different employee groups. For example the finance team do not need to view sizing information.

When we share personal data, we make sure that it remains secure:

- We conduct a data security review of third parties with whom we share personal data to ensure that they will keep your it secure and confidential.
- Every external business we work with is required to have a contract with us which clearly describes our expectations about the way in which they keep personal data secure, the purposes for which they can use personal data and which holds them fully responsible for meeting those expectations.
- We will only send to third parties the personal data that is necessary for the purposes for which it is required.

System Security Measures

To prevent the leaking of data to unauthorised sources and the protection of our systems from cyber-attacks we have a number of security measures in place, as follows:

Perimeter Firewall

This is the main defence of the perimeter of our private network. It is used to detect and protect the network from unwanted traffic, potentially dangerous content and intrusion attempts and to flag up these threats to the network administrator.

Our perimeter firewall blocks incoming network traffic from accessing internal networks and hosts and bars outgoing traffic from accessing undesirable external networks and hosts.

System Update Policy

To ensure that our systems are protected with the latest software updates we have a “System Update Policy” in place to check for updates. We use the following methods to determine when the updates should be performed:

- Review of posted security flaws and patches for each type of update applicable to the computer system.
- An automatic scanning of the system to determine available updates not yet applied to the system or application.

Following the identification of updates, an evaluation is carried out on each one to determine if they would be beneficial to the systems to which the updates are available.

If the updates are deemed beneficial, they are installed. The monitoring and installation of updates is carried out monthly.

Anti-Virus Software

All our systems have managed anti-virus software in place. The software automatically carries out regular scans and updates to combat the latest edition of malware, and flags any detections or issues on our managed cloud portal. New updates are released every hour to minimise the risk of the systems becoming infected.

Training

All our staff are required to complete IT Security Awareness Training online, provided by KnowBe4. In addition to the training we carry out simulated phishing email tests on an ongoing basis to identify any potential weakness and to recommend additional training where required.

Wardrobe Management System Security

In order further to protect our Wardrobe Management System that we have enabled for clients, we have put in place an extra layer of external security. This service is provided by an external contractor and acts as a gateway for internet traffic into the website. This provides an additional firewall which protects the site from external sources or malicious requests. The contractor will also provide regular and scheduled site monitoring and penetration testing to find any areas of vulnerability to possible attack which we will then immediately act upon.

Audit and Review

There is an annual review and audit of the system security measures.

CCTV Cameras

Burlington Uniforms employs CCTV cameras on its premises for the security of its real, personal or intellectual property and for the protection of its employees, visitors and contractors.

CCTV inevitably captures and records the activity and movement of staff and visitors on or about the premises at all times.

Information that CCTV cameras are in use is displayed as appropriate.

Requests for information about images captured on CCTV will be provided on reasonable request. Disclosure of images captured on CCTV will be made for the detection of those suspected of committing criminal offences, in the prosecution of alleged offenders and where disclosure is required in civil proceedings.

Care is taken to ensure that CCTV does not capture images of or on land falling outside the curtilage of the premises.

Signed: 

Date: 19th July 2024
Review Date: 18th July 2025

Adrian Hewitt
Managing Director