ISMS POLICY

PRIVACY POLICY

BELL GLOBAL PROPERTY SERVICES LIMITED

PRIVACY POLICY

Table of Contents

This Privacy Notice applies to all Employees, Subcontractors, Suppliers, Clients and Customers and all other Stakeholders working on behalf of, or in collaboration with Bell Global Property Services (UK) Ltd and all other Bell Group Companies including wholly owned trading subsidiaries such as Bell Group Ltd, CB Contracts (N.I.) Limited, and Paint My Home by Bell Limited, hereinafter all referred to as "Bell".

1 Introduction

The collection of personal data in the UK is regulated by the UK's current Data Protection Legislation namely the UK GDPR and the Data Protection Act 2018.

Bell Global Property Services (UK) Ltd (ICO Registration No. ZB689127), Bell Group Ltd (ICO Registration Number ZA056079) and C.B. Contracts (N.I.) Ltd (ICO Registration No. ZA480144) are registered as Data Controllers with the Information Commissioners Office. They are Joint Controllers of all the data we hold.

They collect necessary personal data via their own procedures and, when necessary, from other Bell Group Companies or third parties who provide information to them or act on their instructions in the collection and processing of personal data.

As our valued employees, apprentices, clients, customers, subcontractors, and suppliers, we want to keep you up to date with the steps Bell is taking to demonstrate our compliance with the UK General Data Protection Regulations (UK GDPR) and the Data Protection Act 2018.

This legislation imposes additional obligations on organisations and gives individuals extra rights around how your personal data is used.

Looking after the personal information you share with us is very important. We want you to be confident that your personal data is kept safely and securely and to understand how we use it to offer a better and more personalised delivery of our services.

It is our goal to be as open and transparent as possible and this Data Protection and Information Security Policy (Privacy Notice) provides more information on the data we hold, what we do with that data, who we share the data with and your rights under UK GDPR.

If we make changes to our Privacy Policy, we will notify you by updating it on our website.

Our point of contact for all Data Protection related matters is via Bell Global Property Services (UK) Ltd.

Should you need to contact us, please write to our Head of Human Resources and Data Protection Champion: Paramjit Kaur, Bell Global Property Services (UK) Limited, Bell Business Park, Rochsolloch Road, Airdrie, Lanarkshire, Scotland, ML6 9BG. Email: HR@bellgroup.co.uk quoting Security and Privacy Enquiry.

2 Data Protection Principles

Bell is committed to complying with data protection law and principles, the "Data Protection Principles" which means we pledge that your data will be:

- Processed lawfully, fairly and in a transparent way.
- Collected and processed for specific, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and kept up to date.
- Kept only as long as necessary for the purposes we have told you about.
- Kept securely and disposed of securely.

Further, that as the data controller we shall be responsible for and able to demonstrate compliance with our duties under the UK GDPR and Data Protection Act 2018.

3 Our Authority to Collect Information

UK GDPR states that we are allowed to collect and process your personal data where we have one of the following legitimate reasons to do so:

- Contract - your personal information is processed in order to fulfil a contractual arrangement e.g. in order to arrange access to carry out maintenance repairs to your premises.
- Consent – where you agree to us using your information for a specific purpose.
- Legitimate Interests – where the processing is necessary for the legitimate interests pursued by us or a third party such as allowing us to provide you with the best products and service in the most secure and appropriate way e.g. for safeguarding residents in sheltered housing. Or for operating back office and administration services in connection with the provision of our services.

Generally, our Legitimate Interests will extend to and cover most situations where we process data except where these interests are overridden by the interests, rights, and freedoms of the data subject. If the data that we process is Special Category Data, such as information relating to health, additional needs, racial or ethnic origins, religious or philosophical beliefs, then we may need to meet additional criteria, such as obtaining or ensuring that we have your consent to process your data.

- Legal Obligation – where there is statutory or other legal requirement to share the information e.g. for law enforcement purposes, HMRC, DWP, Disclosure Scotland, DBS and the HSE
- Vital Interests – where the processing is necessary to protect someone's life.
- Public Interest- where the processing is necessary for us to perform a task in the public interest or for our official functions provided that the task or function has a clear basis in law.
- External providers from whom employees receive benefits and other services such as insurance companies for the death in service benefit, Occupational Health, Drug and Alcohol Testing centres, Royal London and the People's Pension and competence schemes such as CSCS, IPAF, PASMA and Sentinel.
- Social media and marketing purposes unless you advise us in writing that you do not wish to appear in any social media posts or any marketing material.

<u>Please note that the information we collect depends on the nature of our relationship with you.</u>

4 Clients and Customers/Residents and other End Users

4.1 What information do we collect?

Due to the nature of our work, we collect information on Clients and Customers / Residents to identify the preferred method of communication or special needs or arrangements. This can be information such as.

- Full name
- Address
- Contact numbers
- Email address.
- Details of special circumstances or requirements, such as disability or religious needs
- Background information such as medical conditions or criminal history

4.2 How do we collect information?

When entering into a new agreement or new phase of an existing contract, we will usually ask our client to provide some personal information concerning their employees, customers, residents, or end users who are involved in the contract or are to receive work to their properties.

Throughout the duration of our project, in line with our clients' requirements, we will be engaged directly in contact with customers / residents and others involved in the contract works in person. To ensure optimum service delivery we will continually update information on customers, residents and involved parties' needs. This can be using:

- Information collected before planned improvement work from our Clients
- Feedback from our operatives on site
- Information provided as part of the customer or client satisfaction questionnaires.
- Information collected via site progress or management meetings
- Information provided by the Client such as required security processes.

4.3 Why do we collect information?

We collect all such data for the necessary and effective provision of our services; carrying out repairs, refurbishment, replacement, maintenance, and redecoration works to all forms of occupied properties. Bell is a family owned and operated business and our main objective is to make certain we tailor our service considering all relevant factors when planning our work and customer care approach.

The personal data we receive in relation to the contract works we undertake is essential to assisting us in providing an efficient and second-to-none service. As such, we may need to share any relevant personal information we hold on clients, end users / customers / residents to the project team employees as a matter of safeguarding all parties concerned. As a business, we have a duty of care to our employees as well as to others such as clients and customers and our Company Policies provide guidelines to ensure the safety of all individuals affected by the works in progress.

5 Employees and Contractors

5.1 What information do we collect?

During your contract of employment, apprenticeship, or service agreement with Bell, we will collect, store, and use personal information such as.

- The information you have provided to us in your curriculum vitae and covering letter or within an application form.
- The information you have provided to us in your Supplier Approval Questionnaire. The information you have provided on our Employee Starter Form, including name, address, telephone number, personal email address, date of birth, National Insurance number, contact details for your emergency contact(s), bank details for the purposes of processing your wages/salary, employment history and qualifications.
- Any ID provided during the onboarding process such as a copy of your passport and driving licence.
- Any information you provide to us during an interview.
- We may also collect, store, and use the following types of more sensitive personal information:
- Information about your race or ethnicity, or religious beliefs.
- Information about your health, including any medical condition and/or disability, , and sickness records.
- Information about your sexual orientation.
- Information about criminal convictions and offences which forms part of our onboarding process.

5.2 How do we collect information?

- We collect your personal information from the following sources:
- From you directly, the employee, apprentice, or suppliers, as listed above – e.g. interview, employee or apprenticeship starter form, Approval Questionnaire, via SSIP subscription, Equality questionnaire.
- Recruitment agencies or from your college and Bell Academies
- Disclosure and Barring Service in respect of criminal convictions.
- Your named referees, from whom we collect the following categories of data: your dates of employment or previous studies; your role with the referee (if applicable); summary of your performance (if applicable).
- Third parties from a publicly accessible source: social media sites such as LinkedIn, Facebook, and Twitter.

5.3 Why do we collect this personal information?

We collect your personal data and background information for the following main reasons:

1. Recruitment, promotion, human resources, training, fleet management and payroll.
2. effectively managing our people and processes to ensure we are a fair and equal opportunities employer; for instance, if we can make reasonable adjustments in response to a disability or religious needs.
3. We are required to carry out criminal records check to satisfy ourselves that there is nothing in your criminal convictions history which makes you unsuitable for your role within Bell. We often work in areas of high security and our clients require adequate background checks to be made to attain relevant access.
4. to streamline our operations in the effective provision of our services; carrying out repairs, refurbishment, replacement, maintenance, and redecoration works to all forms of occupied and void properties.
5. To comply with legal and regulatory requirements
6. So that employees may receive certain benefits and entitlements such as sick pay, healthcare, pensions, death in service.

6 Management of Data

All data held by Bell is secured and is stored under the standards and requirements of the UK GDPR and Data Protection Act 2018. We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used, or accessed in an unauthorised way, altered, or disclosed.

We have anti-virus, firewalls, malware, and anti-spyware software on every computer used by Bell and the software is frequently updated. All Bell offices are connected via a Wide Area Network, which works using a 128bit encryption through a Private VPN tunnel which doesn't touch the public internet, making all data sent virtually invisible.

Bell documents and information in our possession includes, but is not limited to:

- Personnel files including contact details, ID and Equality and Diversity data
- Training records
- Payroll and bank details
- Group Policies and Bid Library
- Any Court Orders received regarding a mandatory deduction of wages
- Financial and accounting information inherent to all departments and divisions of Bell
- Sales and BDM database including client details, enquiry history and contacts
- Tender documents, contracts and final invoices
- Other contract information provided by our clients, including intellectual property such as drawings or security information
- Data received from customers including contact information or special circumstances

Throughout all branches, we utilise a document management system, which specialises in electronic filing within our Company Intranet. The system minimises the generation of paperwork aiding faster efficient information sharing and access between Company employees and project team members. Our IMS is available to all Bell employees although it is password secured with the use of different levels of access to ascertain that document folders can be accessed only by those who require that particular information solely for work purposes. The password-controlled entry is tightly controlled by our Director of IT and Board of Directors and as a result, the document store is secure, and protected. Access is granted via mapped drives and each user can only physically see the data they are allowed access to. Two (2) Factor Authentication is also turned on therefore every user must authenticate their access on two levels, not just through a password.

Office and Contracts staff are subject to a contractual duty of confidentiality shall only process personal information according to management instruction.

All data controlled and processed by the company is held on main servers within a solid brick room formerly used as an armoury. The data is both encrypted but also password protected. The servers are virtualised thus allowing Bell

to run several software platforms on one physical hardware server, resulting in less of a carbon footprint. Data is further protected by way of utilising the virtual servers in off-site locations. Data is backed up between servers every 15 minutes across fibre data links between sites using backup software and Microsoft's own replication which is built into many of their software server platforms. If we have any problems with hardware disks in the servers these can be 'hot' replaced and the physical server will rebuild itself, as there are always at least two physical disks in each machine which are redundant to allow for failover. Therefore, in the event of any problems to our servers there is always at least one available for continuity.

All financial software held by Bell is maintained, hosted, and supported by the software award winning company Eque2.

Any necessary removal of data whether in hard or electronic copy is protected and also tracked. The printout and use of copiers is locked down and is tracked via software and the use of USBs and other electronic devices are also controlled by our IT team who run endpoint protection software. PCs and laptops have their USB ports locked down, and only opened once a formal change request has been actioned and then they are monitored to see what information is added or removed from within Bell IT system, whether from a mapped drive or a desktop therefore making it harder to steal or remove data.

7 The Support Systems We Have in Place to Enable the Ongoing Integrity of Personal Data

Our Company does not require the services of a Data Protection Officer; however, we have put in place 7 Data Protection Champions throughout Bell who are senior managers, have attended management training on GDPR and have the responsibility of ensuring effective Data Protection within their own departments. As a second tier we have 12 Privacy Representatives UK-wide, who liaise with the DPCs to ensure processes, policies and procedures are implemented effectively at local level within their respective branches.

8 Data Breach

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

This is managed by our Director of I.T. and Head of Human Resources. Our Head of HR is the nominated champion for managing subject access requests, reporting of breaches and all other legal documentation pertaining to the new regulations.

Office and Contracts staff shall only process personal information according to management instructions.

9 Monitoring of Communication Resources

Our Director of IT is responsible for the day-to-day monitoring of the use of communication resources, such as mobile phones, tablets, photocopiers / scanners, email, Internet, and Intranet use. In addition, our Internal Auditors undertake a monitoring role to ensure that this policy is being applied within their nominated branch(es).

10 Who We May Share your Information with and why

Bell works with a limited number of external parties with whom it is necessary to share your data. These would generally include the following:

10.1 Colleges and Training Providers

External parties who provide services on behalf of the company to our apprentices and employees. These may include colleges, training providers and iHasco online partners.

10.2 Auditors

In line with our commitment to ensure that we have the most effective processes and policies in place and ensuring compliance, we may from time to time, be audited by any relevant regulatory body or an external provider that specialises in auditing businesses to ensure that our working practices are of the highest standard. During these audits, Bell may be asked to demonstrate how it follows a particular process and provide examples of where it was implemented. As such, the Company may share your personal data with the auditor where necessary. Auditors are required to treat your personal data in the same manner that we do.

10.3 Supplier Partners

Bell works with a limited number of trusted partners and contractors who supply products and services on our behalf. All partners are subject to security checks and will only hold the necessary amount of personal information needed to fulfil work orders or provide specialist services to individual properties or projects on our behalf.

10.4 Delivery Partners

For our project teams to receive goods in carrying out our service, Bell works with several delivery partners. We only pass limited information to them to ensure delivery of items.

10.5 IT Companies

Bell works with companies who support our website and other business systems, including Eque2 who host all financial and accounting data as well as our payroll, purchase, and sales ledgers.

10.6 Marketing Companies and Printers

We work with a few marketing companies who help us manage our corporate marketing material, but we do not foresee that this would involve any personal information. Only in some cases would this involve publishing photographs of our employees during work activities. We would always attain permission from our employees, client, and customers prior to arranging this.

10.7 Payment Processing

In a small number of Bell premises where we have a Decorator's Centre, we work with trusted third parties to securely take and manage payments.

10.8 Customers

Names and contact details of our project team members may be issued to customers for the effective management of a project, to coordinate access and to ensure the security of all parties involved – e.g., to avoid unauthorised access by unwanted individuals or rogue traders.

10.9 Clients

Due to the size and nature of our business, the tendering process for being awarded work usually involves our bid team submitting a large quantity of information on past projects. In these instances, we may send photos of our operatives working, or of works we have carried out or even case studies on previous works or community projects. In addition, we may need to share general information on our employees including Equality and Diversity Statistics for regional offices or Qualifications of operatives and staff to be deployed on specific contracts. This will generally not require Special Category Data to be disclosed about any individual, but if this is necessary Bell shall carry out a Data Protection Impact Assessment (DPIA) and obtain your consent before sharing this data.

10.10 George and Annette Bell Foundation

We have partnered with and support our Charity Partner the George and Annette Bell Foundation for whom we are privileged to carry out various local community projects. In doing so we share data regarding those employees and contractors who are involved in those projects. In addition, we share data regarding employees who are willing to support the Foundation individually, for example by taking part in the Foundation lottery. The data shared with the

Foundation is processed in accordance with the UK GDPR and Data Protection Act 2018 and involves the same rigorous controls and security that are employed by Bell.

11 Transfers to Third Countries

Bell does not transfer any personal data outside of the U.K. Nor does it use any data centres that are not in the UK to hold its data.

12 Keeping in touch with you

12.1 Employees, Apprentices and Contractors

To be a successful business, it is essential that we maintain an effective communication flow across all roles and between branches. All employees, apprentices and contractors working on our behalf have a legal obligation to adhere to the Company's systems of work as outlined in our Policies and Procedures and in accordance with instructions provided by Bell Managers. All employees, apprentices and contractors are obliged to use the information they have gained in training to produce an optimum quality of work whilst looking after the wellbeing of themselves and those affected by their work. All employees, apprentices and contractors alike are encouraged to bring to the attention of Bell Managers any information or requirements they feel will assist in the implementation of the Company's Policies.

Employee, apprentices, and contractor feedback is highly valued and when received in whatever form, it is recorded and acted upon by Senior Management. Our Bell mobile platform and portal provides a vessel for direct communication flow between departments and employees in any location or role, which inevitably facilitates our goal in achieving a high standard of operations within all our premises and sites. To that effect, we encourage and are hugely grateful to all employees and apprentices who provide us with personal data such as a personal email address. Information pertaining to your work is usually transferred electronically and this will aid good communication.

12.2 Clients

With our clients it is essential that we maintain an effective communication flow between all parties involved in any awarded contract. To that effect we shall create a communication network prior to commencement and keep in touch with all client personnel in relation to the operations being undertaken on your behalf. Information from and to our clients is usually transferred electronically, which may include personal data such as personal contact details, financial data and personal data pertaining to you or your customers including Special Category Data or special circumstances. We will not share this information with parties outside of Bell or with those who are not involved in the contract without your permission or unless we have a legal basis to do so.

12.3 Customers/Residents

For customers, we want to keep you up to date with information about our services and social value within your community. We may do this initially through paper correspondence and subsequently, depending on agreement, permissions, or legal basis, via telephone or email. The reason for our communication is solely to inform you of our forthcoming visits, to arrange access, manage the works, to manage any arising issues or complaints and in some cases to attain your feedback upon completion of the work.

However, if you decide you do not want us to contact you, even for work purposes, any individual can request that we stop by writing to our Head of Human Resources and Data Protection Champion at HR@bellgroup.co.uk or by calling your local Bell Branch. All contact details can be obtained from our website www.bellgroup.co.uk.

You may continue to receive mailings for a short period while your request is dealt with.

Please note that if we are unable to contact you or process your personal data that we may not be able to carry out the contract works relating to you or your property.

13 How long we keep your information and Secure Disposal

Following the collection and processing of any required personal data for the purpose of our service delivery and as noted in this Privacy Notice, the length of time we retain it is determined by several factors, including the purpose for which we use that information and our obligations under other laws.

We may need to retain personal data for auditing purposes or to establish, bring or defend legal claims. For this purpose, we will always retain project specific data including personal data for 7 years after the date of completion of work.

Any personal data pertaining to residents, customers or building end users, such as names, phone numbers or vulnerable status, will be securely destroyed when no longer required. (please see the paragraph above). This will usually be within 90 calendar days after any applicable law or legal basis which requires Bell to continue to store such Personal Data.

The only exceptions to this are where:

- the law requires us to hold your personal information for a longer period or delete it sooner.
- you exercise your right to have the information erased (where it applies) and we do not need to hold it in connection with any of the reasons permitted or required under the law.
- we bring or defend a legal claim or other proceedings during the period we retain your personal data, in which case we will retain your personal data until those proceedings have concluded, and no further appeals are possible; or
- in limited cases, existing or future law or a court or regulator requires us to keep your personal information for a longer or shorter period.
- As per any contractual obligation, again data will be destroyed within 90 days of the end of a contract unless defined in the contract.

We use retention policies within Bell's SharePoint sites

If the data is on the server we use the Symantec PGP software, which works by overwriting data with random text multiple times, making it impossible to recover.

For hard copy data, all office staff and contract staff know to utilise the bins provided in our office premises for any sensitive data. The bins are managed by Shred-IT and are locked to prevent unauthorised access. Shred-IT attend our premises at regular intervals to securely shred and destroy all data within the bins.

14 What are your rights?

In line with the Information Commissioner's Office Data Sharing Code of Practice, Bell commits to adopting the good practice recommendations outlined within the guidelines. You are entitled to request the following from Bell, these are called your Data Subject Rights and there is more information on these on the Information Commissioners website www.ico.org.uk

- Right of access –to request access to your personal information and information about how we process it
- Right to rectification –to have your personal information corrected if it is inaccurate and to have incomplete personal information completed
- Right to erasure (also known as the Right to be Forgotten) – to have your personal information erased. Contact our Head of Human Resources and Data Protection Champion on HR@bellgroup.co.uk / 01236 766878
- Right to restriction of processing – to restrict Bell processing your personal information
- Right to data portability - to electronically move, copy or transfer your personal information in a standard form
- Right to object to processing of your personal information
- Rights with regards to automated individual decision making, including profiling

If you have any general questions or requests about your rights, please contact HR@bellgroup.co.uk. The information will be provided within 30 days of the date of the request free of charge.

Similarly, if you believe that your data is being used in a way that is not compliant with the UK GDPR and the Data Protection Act 2018 then you can complain to Bell by contacting the HR Department as noted in this Privacy Notice and we will seek to resolve any issues or concerns you may have.

We will respond initially to your complaint within 1 month.

Following this procedure, you may complain to the Information Commissioners Office (ICO), who is the Data Protection Regulator in the UK. Their details are available at www.ico.org.uk

15 Contact

Should you need to contact us please write to our Head of Human Resources and Data Protection Champion: Paramjit Kaur, Bell Global Property Services (UK) Ltd, Bell Business Park, Rochsolloch Road, Airdrie, Lanarkshire, Scotland, ML6 9BG.

Email via HR@bellgroup.co.uk quoting Security and Privacy Enquiry.

For and on behalf of Bell Global Property Services (UK) Ltd and all wholly owned subsidiaries, including: - Bell Group Ltd, CB Contracts (NI) Ltd, PMH by Bell Ltd.