DATA PROTECTION AND INFORMATION SECURITY POLICY

Issued 25th May 2018

Privacy Notice 25th May 2018

To all Employees, Suppliers, Clients and Customers and any other Stakeholders working on behalf of, or in collaboration with, Bell Group U.K. Limited (hereon in referred to as "Bell Group"), including all wholly owned subsidiaries; Bell Decorating Group Limited, P&D Scotland Limited, Torbay Decorating Company Limited, Abco Management Limited John Miller & Sons Limited and Cyril John Limited.

As our valued employees, clients, customers and suppliers, we want to keep you up to date with the steps Bell Group is taking to demonstrate our commitment to complying with the General Data Protection Regulations and the Data Protection Act 2018, which has come in to effect as of the 25th May 2018. GDPR imposes additional obligations on organisations and gives individuals extra rights around how your 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 service.

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

If we make changes to our Privacy Policy, we will notify you by updating it on our website. Should you need to contact us, please write to our HR Manager and Data Protection Champion:

Paramjit Barry, Bell Group UK Limited, 130 Pitt Street, Edinburgh, EH6 4DE
Email via HR@bellgroup.co.uk quoting Security and Privacy Enquiry.

Kind Regards,

The Bell Group Data Protection Team

DATA PROTECTION AND INFORMATION SECURITY POLICY

Issued 25th May 2018

Introduction

Bell Group is registered under current Data Protection Legislation enacted in the U.K. in respect of the protection of personal data, meaning: Regulation (EU) 2016/679 (GDPR 2018) and any national implementing laws, regulations, secondary legislation as well as guidance and codes of practice issued by the Information Commissioner. Our Registration Number is: **Z2933329.** This register entry includes data being processed and retained by Bell Group for various purposes including:

1. Staff Administration, Payroll and Human Resources
2. Advertising, Marketing and Public Relations
3. Accounts and Finance records
4. Sales and Business Development
5. Crime Prevention and Personnel Security.
6. Customer liaison and effective customer care procedures
7. Contract Management and Client communications

All information is maintained within the stated guidelines of GDPR and Data Protection Act 2018 and all employees of Bell Group have received training relevant to their role in relation to compliance with the regulations.

Data Protection Principles

Bell Group is fully committed to complying with data protection law and principles, which means we pledge that your data will be:

- Used lawfully, fairly and in a transparent way.
- Collected only for valid purposes directly in relation to the main purposes of running our business operations and not used in any way that is incompatible with those purposes.
- Kept up to date.
- Kept only as long as necessary for the purposes we have told you about.
- Kept securely.

CLIENTS AND CUSTOMERS

What information we collect and why?

GDPR states that our Company is allowed to use and share your personal data where we have one of the following ligitimate 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 in this way, such as providing addresses to certain third party partners for delivery of goods or specialist services to assist in our contract.

- Legitimate Interests - 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.
- Legal Obligation – where there is statutory or other legal requirement to share the information e.g. for law enforcement purposes.

Due to the nature of our work, very little external data is stored from client sources. We do however collect information on customers to identify particular needs and the preferred method of communication. When entering in to a new agreement or new phase of an existing contract, we will ask our Client to provide some personal information concerning the customers, residents or end users to receive work to their properties 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

Throughout the duration of our project, in line with our clients' requirements, we will be engaged directly in contact with customers in person. We build a profile of customers through various formats and sources to ensure optimum service delivery and we will continually update information on customer needs using:

- information collected before planned improvement work from client database
- feedback from our operatives on site
- information provided as part of the customer or client satisfaction questionnaires
- information collated via site progress or management meetings
- information provided by the Client such as required security processes

We collect all such data for the effective provision of our services; carrying out repairs, refurbishment, replacement, maintenance and redecoration works to all forms of occupied properties. Bell Group 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 customer care approach.

The personal data we receive in relation to the Contract of Work, goes a long way to assisting us in providing a second to none service. As such, we see fit to disclose any relevant personal information on 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 clients and customers and our Company Policies provide guidelines to ensure the safety of all individuals affected by the works in progress.

We will work collaboratively with customer, resident representatives, community groups and relevant client staff members to ensure our means our capturing, maintaining and storing information is entirely compliant with our equality and diversity policies and GDPR 2018.

Operatives are instructed of particular circumstances on a daily basis through site induction and that information cannot be accessed by any individual other than those authorised project personnel and RLOs dealing with the specific property. Following completion of any site, it is the responsibility of our Project Manager to destroy all sensitive data, which is shredded at office premises. Only relevant feedback, questionnaires and site inspection are retained, which are stored under our password protected management system.

EMPLOYEES AND CONTRACTORS

What information we collect

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

- The information you have provided to us in your curriculum vitae and covering letter or within an apllication to work 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 next of kin, employment history and qualifications.
- Any information you provide to us during an interview.
- Details of special circumstances or requirements, such as adaptations for a disability

We may also collect, store and use the following types of more sensitive personal information:

- Information about your race or ethnicity, religious beliefs and sexual orientation.
- Information about your health, including any medical condition, health and sickness records.
- Information about criminal convictions and offences.

How Is Your Personal Information Collected?

- We collect your personal information from the following sources:
- From you directly, the employee or suppliers, as listed above – e.g. interview, employee starter form, Approval Questionnaire, via SSIP subscription, Equality questionnaire.
- Recruitment agencies
- 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; your role with the referee (if applicable); brief summary of your performance (if applicable).
- Third parties from a publicly accessible source: social media sites such as LinkedIn, Facebook and Twitter.

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 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 a criminal records check in order 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 in order to attain the 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

Within Bell, we commit to:

- ✓ Forming a stable working environment for our employees, which encourages a long-term career path and personal development
- ✓ Training for all employees of every level within the Organisation
- ✓ Encouraging feedback from our employees to make improvements to our business strategy
- ✓ Investing in Social Dividend and developing skills within the communities where we work
- ✓ Actively encouraging a positive working environment free from harassment, bullying and any form of discrimination.
- ✓ Ensuring that everyone receives equal treatment.
- ✓ Employing people who reflect the diverse communities within which we work
- ✓ Ensuring all employees are made aware of our policies and practices to encourage positive behaviour.
- ✓ Listening and acting upon peoples' views to improve the working environment.

We strive to maintain a family ethos in terms of; community investment, respect for people and long-term career development of our employees. We value our employees' backgrounds, opinions and wellbeing and truly believe that your input and feedback is important in forming a successful business. Inherent to this, it is necessary to collate data and personal information to allow us to realise our aims and objectives, to shape our business strategy and be the best employer we possibly can be.

Management of Data

The technical and organisational measures we have in place to ensure that personal data is stored securely and protected against accidental, unauthorised or unlawful destruction, loss, alteration, disclosure or access

All data held by Bell Group is secured and is stored under the standards and requirements of GDPR 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. Our IT Manager has anti-virus, firewalls and anti-spyware software on every computer used by Bell Group and the software is frequently updated. All Bell Group offices are connected via a Wide Area Network, which works using a 128bit encryption through a VPN tunnel over the Internet, making all data sent virtually invisible.

All Group documents and contract information in our possession includes, but is not limited to:

- Personnel files including contact details, ID and Equality and Diversity statistics
- Training records
- Payroll and bank details
- Group Policies and Bid Library
- Financial and accounting information inherent to all departments and divisions of Bell Group
- 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 Concept's INVU document management system, which specialises in electronic filing within our Company Intranet. All of the above information is retained electronically and strictly accessible via INVU controls. 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 Group employees although 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 IT Manager and Board of Directors and as a result, the document store is secure, protected and trouble free. Access is granted via mapped drives and each user can only physically see the data they are allowed access to.

Office and Contracts staff shall only process personal information according to management instruction and they are subject to a duty of confidentiality. Details of these measures may be obtained from our H.R. Manager. 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.

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 Group to run several software platforms on one physical hardware server, resulting in less of a carbon footprint and data 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 also 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 Group is maintained, hosted and supported by the software award winning company Redsky IT. Redsky hosts in the cloud our financial software package Summit 3000, which is accessible across the internet and is again 128 bit encrypted and also password protected, with users only being able to see the data that is pertaining to their job. Redsky backup our server to various data centres across the world. All data is held in accordance with the data protection act.

The removal of data whether in hard or electronic copy is protected and also tracked, the print out 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. PCs and laptops have their USB ports monitored to see what information is added or removed from within Bell Groups IT system, whether from a mapped drive or a desktop therefore making it harder to steal or remove data.

The support systems we have in place to enable the ongoing integrity of personal data

Our Company does not require the services of a DPO, however we have put in place 7 Data Protection Champions throughout the Group 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.

Three of Bell Group's senior managers in particular have taken the lead in managing our GDPR strategy to ensure the continued integrity and security of all personal data we process and control. Bell Group's IT Manager oversees all communication and software security and advises the Board on investments inherent to maximising our efficiency and effectiveness in data protection. Our National Quality Manager, one of our nominated DPCs, in responsible for developing and implementing a Data Protection Strategy Group-wide, liaising regularly with departmental managers and administration support teams to implement good practice in line with GDPR requirements throughout all Company activities. Our Human Resources Manager is a qualified lawyer who specialised in employment law with a leading commercial law firm for 8 years before joining Bell Group. Our HR Manager is the nominated champion for managing subject access requests, reporting of breaches and all other legal documentation pertaining to the new regulations. Both Managers attended the GDPR:Summit London supported by Henley Business School, University of Reading and sponsored by IBM on the 23rd April.

Monitoring of Communication Resources

The IT Manager is responsible for the day-to-day monitoring of the use of communication resources, such as mobile phones, tablets, photocopiers / scan file, fax, email, Internet and Intranet use. In addition, our 12 Internal Auditors undertake a monitoring role to ensure that this policy is being applied within their nominated branch(es).

a) All electronic data is protected against fires, floods, etc. by a backup system at an external server, which stores a backup copy of all electronic documents
b) Our ISP Highnet backs up all emails coming in and out of the Company in relation to anti-terrorist laws and Redsky IT hosts and protects our financial software Summit 3000.

Who we may share your information with and why

Bell Group works with a very limited number of external sources with whom we are required to share your data. These would generally only concern the following:

Supplier Partners

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

Delivery Partners

In order for our project teams to receive goods in carrying out our service, Bell Group works with a number of delivery partners. We only pass limited information to them in order to ensure delivery of items and this would never include personal names or contact details – only an address.

IT Companies

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

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.

Payment processing

In a small number of Bell Group premises where we have a Decorator's Centre, we work with trusted third parties in order to securely take and manage payments. In addition, our business bank accounts are managed by HSBC and your payment details will be recorded within HSBC's secure systems.

Customers

Names and contact details of our project team members 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.

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, information such as values and specification of works we have carried out or even case studies on community projects. In addition, we agree 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 sensitive information to be disclosed about any individual, but more as a Group. Bell Group shall carry out a risk assessment before sharing any personal data with any current or potential client to monitor the relevance and potential consequences of sharing such information, and this shall be monitored by senior management before being issued to ensure we continue to adhere to the Code of Practice as well as The Data Protection Act.

Transfers to third countries

Bell Group does not transfer any personal data outside of the U.K.

Keeping in touch with you

EMPLOYEES 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 and contractors working on our behalf have a moral and 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 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 and contractors alike are encouraged to bring to the attention of Bell Group Managers any information or requirements they feel will assist in the implementation of the Company's Policies.

Employee and Contractor feedback is highly valued and when received in whatever form, it is recorded and acted upon by Senior Management. Our Bell App 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 who provide us with a personal email address. Information pertaining to your work is usually transferred electronically and this will aid good communication. We will not share your correspondence or personal details with any individual external to Bell Group who is not directly involved in managing your work activities, without your prior permission.

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 with our clients is usually transferred electronically, which may include; personal contact details, financial data and information pertaining to your customers such as

sensitive data or special circumstances. We will not share your information with companies outside of Bell Group or who are not involved in the contract without your permission.

CUSTOMERS - For customers, we want to keep you up to date with information about our services and social value within your community. We will do this initially through paper correspondence and subsequently, depending on permissions granted, via telephone or email. The reasons 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 HR Manager and Data Protection Champion at HR@bellgroup.co.uk or by calling your local Bell Group 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.

How long we keep your information

If we collate and file any sensitive, financial, personal or contractual information relating to our employees, contractors, suppliers, clients and customers or other data received from external sources, the length of time we retain it is determined by a number of factors, including the purpose for which we use that information and our obligations under other laws.
We may need your personal information for auditing or legal reasons. For this purpose, we will always retain your personal information for 7 years after the date it is no longer needed by us for any of the purposes listed under "How do we use your information" above. 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 information, in which case we will retain your personal information 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.

What are your rights?

In line with the Information Commissioner's Office Data Sharing Code of Practice, Bell Group commits to adopting the good practice recommendations outlined within the guidelines. You are entitled to request the following from Bell Group, 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 H.R. Manager on HR@bellgroup.co.uk / 0131 553 3747
- Right to restriction of processing – to restrict Bell Group 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

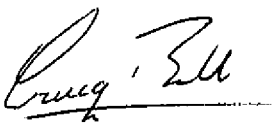
If you have any general questions about your rights or want to exercise your rights please contact HR@bellgroup.co.uk . The information will be provided within 30 days of the date of the request free of charge.

You have the right to lodge a complaint with a data protection regulator in Europe, in particular in a country where you work or live or where your legal rights have been infringed. The contact details for the Information Commissioner's Office (ICO), the data protection regulator in the UK, are available on the ICO website www.ico.org.uk. Where your personal information has or is being used in a way that you believe does not comply with GDPR, we encourage you to contact Bell Group's HR Department before making any complaint and we will seek to resolve any issues or concerns you may have.

Contact

Should you need to contact us please write to our HR Manager and Data Protection Champion:
Paramjit Barry, Bell Group UK Limited, 130 Pitt Street, Edinburgh, EH6 4DE
Email via HR@bellgroup.co.uk quoting Security and Privacy Enquiry.

For and on behalf of Bell Group U.K. –
Chief Executive, Craig Bell



Reviewed: 25th May 2018
Review Date: 25th May 2019

(BELL GROUP UK AND ALL WHOLLY OWNED SUBSIDIARIES INCLUDING;
BELL DECORATING GROUP LIMITED, P&D SCOTLAND LIMITED, TORBAY DECORATING COMPANY LIMITED, ABCO MANAGEMENT LIMITED, CYRIL JOHN LIMITED, JOHN MILLER AND SONS LIMITED)