

## **Data Protection, GDPR, Confidentiality and Security Policy**

Owned by	Will Smith, Managing Director
Reviewed	July 2019
Version	5
Next Review Date	July 2020

### **Introduction**

Smith & Byford is committed to fulfilling its legal obligations within the provisions of the Data Protection Act 1998 and the Freedom of Information Act 2010 and have taken appropriate measures to keep client and employee information safe and secure. We collect personal information about our employees and work with our clients to receive limited personal data about residents.

We strive to comply at all times with the principles of the Data Protection Act 1998, which places obligations on organisations, such as our clients, and protects the rights and freedoms of the individuals who are subjects of that data.

### **Data Protection principles**

#### The Data Protection Principles

There are a number of Data Protection principles that must be adhered to. The following is a summary:

1. Personal data shall be processed fairly and lawfully and in particular, shall not be processed unless specific conditions are met;
2. Personal data shall be obtained only for one or more specified and lawful purposes;
3. Personal data shall be adequate, relevant and not excessive;
4. Personal data shall be accurate and where necessary kept up-to-date;
5. Personal data shall not be kept for longer than is necessary;
6. Personal data shall be processed in accordance with the rights of the data subject;
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction or, or damage to personal data;
8. Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures adequate levels of protection for the rights and freedoms of the data subject in relation to the processing of personal data.

Smith and Byford Limited, St George House, Station Approach, Cheam, Surrey, SM2 7AT  
 Reg. No. 1074356 England, Registered Office St George House, Station Approach, Cheam, Surrey, SM2 7AT  
 Directors: W.Smith, D.Ovington, A.Wilson, P.McLachlan, B.Grove, B.Smith, H.Smith, M.Herridge



## **GDPR**

Smith and Byford are fully GDPR compliant and as such have taken steps to ensure the security and integrity of data held on our systems and with interchange to external parties.

Smith and Byford do not outsource IT Services to external vendors to store or maintain data. All data is held on our own servers at our own data facilities with secure physical access utilising swipe card and fingerprint access.

Smith and Byford recently undertook additional measures during GDPR exercises to identify, classify and centralise all data. This procedure ensures that we can implement appropriate storage policies for holding, accessing and backing up our data. In addition, we took steps to ensure our access policies are up to date so that data segregation and access permissions are correct.

We have also undertaken steps to ensure staff are trained to handle data safely and correctly, ensuring information is only stored in designated areas on our servers and no information is located on end user devices. Our teams are regularly reminded through internal memos, training and emails to respect and participate in our data safe culture. We understand that this not only extends to data stored on our systems, but also printed materials in our offices. Our password policy enforces regular password changes for staff ensuring appropriate complexity for security.

Our engineers use mobile tablets secured through an SSL link to our database. We do not store any client data on the mobile tablets, instead engineers access a live job sheet from our servers without downloading information to local disk. All mobile devices are secured using local encryption and password, with remote wipe functionality should a device be lost or stolen.

We maintain strict physical and virtual access to our offices and I.T Systems, utilising multi layers of security using industry leading platforms. Remote access to our internal data is restricted to specific team members and utilises 256 bit VPN access through our edge firewalls. In some cases, we also apply MAC address or remote fixed IP Address mapping for external access.

In cases where we utilise remote access to client platforms, we segregate client systems using individual VLAN's with strict access policies. Client links are secured with a 256 bit VPN tunnel and lengthy pre-shared key encryption strings with fixed IP address validation.

To keep our data safe and ensure business continuity we employ two separate data backup technologies providing snapshots throughout the day, and nightly long term retention backup. We also implement endpoint protection on all systems against malware, spyware and viruses.

To ensure our systems continue to remain secure we utilise industry leading Firewall and Security products to protect our data and engage with external partners for annual penetration testing and security reviews. We undertook our most recent penetration test in October 2018, and continue to work with external partners to maintain our security posture.

## **Roles and Responsibilities**

### **Smith and Byford Board**

- Ensure that the Policy is enforced and resourced appropriately
- Undertake leadership and sponsorship of the Policy
- Review the policy on an Annual basis

### **Management Responsibilities**

- Manage, monitor and report on the progress of the Policy and delivery plan as required

## **Employee Responsibilities**

- It is obligatory for staff to sign a confidentiality undertaking form upon commencement of their employment. Staff must also take part in regular training as required. Training is organised and facilitated by the Management Team and our Company Trainer. All training will take place at a time when its effect on our customers or clients is minimal.
- Staff are personally responsible and accountable for ensuring compliance with the principles of the Act

Set out below is our procedure for implementing our policy ensuring that the Data Protection principles are met and our procedures for dealing with any request made under the Freedom of Information Act.

## **1. Management of Data**

All IT systems are protected by firewall technology, which is updated regularly, to prevent any “unauthorised access to, or alteration, disclosure or destruction of, the data against their accidental loss or destruction” Our bespoke web portal is used by clients to receive data and reports. All information is password protected and held on a secure server. In addition Smith & Byford have a policy of signing confidentiality agreements with all clients and adhere to any and all specific instructions made by the client regarding any information provided.

## **2. Personal Data**

Smith & Byford is committed to fulfilling its legal obligations within the provisions of the Data Protection Act and we are aware of the sensitivity of personnel data and have taken appropriate measure to keep client and employee information safe and secure. All hard copies of our personnel records are stored in a lockable cabinet, which the HR director has access too. All electronic copies are stored on our SAGE HR system which is password protected.

In order to ensure effective operation of the equal opportunity policy (and for no other purpose) a record is kept of all employees’ and job applicants’ gender, racial origins and disability. Such records will be analysed regularly and appropriate follow-up action taken. Where necessary, employees will be able to check/correct their own record of these details, otherwise access to this information is strictly restricted.

We adhere to any and all client wishes regarding any personal data collected and ensure at all times that we only collect the personal data that is necessary to fulfil the operational needs of any service provided.

Subject to the exceptions set out below and elsewhere in this procedure, sensitive personal data shall generally only be processed after the employee or client has given express consent. The Company may in certain situations process the data without consent if it is necessary for processing taking place for one of the following purposes:-

- ensuring health and safety of staff;
- ensuring a safe working environment;
- maintaining records of statutory sick pay or maternity pay;
- protecting the person and property of people entering on to the premises of where Smith & Byford are carrying out work;
- Carrying out any other obligation or enforcing any right under employment law.
- Participating in legal proceedings or obtaining legal advice.
- For the administration of justice.
- For medical purposes by a health professional.

Sensitive personal data relating to racial or ethnic origin may be processed without express consent in order to monitor the effectiveness of the Company’s Equality & Diversity Policy and Procedure.

### 3. Requests for Information – Freedom of Information

An employee or client about whom the Company holds personal data has the right to be:

- told whether their personal data is being processed by or on behalf of the Company and, if so, to be given a description of:
  - i. the personal data held;
  - ii. the purposes for which it is being processed and;
  - iii. the recipients of the personal data
- given a copy of the personal data in an intelligible format (unless to do so is disproportionate or the person has agreed to an alternative way of providing access)
- given any information available regarding the source of the personal data

Written requests should be directed to the Director of HR. If you are an employee and you receive a written request then you should forward this to the Director of HR immediately.

The request for information will be dealt with promptly and in any event within 40 days from the Company receiving:

- the written request for the personal data;
- sufficient details to allow the Company to respond to it;
- sufficient details to confirm the identity of the person making the request

Where the provision of information would reveal the identity of a third party, the information may not be provided unless either the consent of that third party is obtained or it is reasonable to proceed without their consent.

### 4. Document Retention and Destruction

This policy provides for the systematic review, retention and destruction of documents received or created by Smith & Byford. Documents are held for a maximum of 7 years (unless relating to employees who are currently employed by S&B). Documentation relating to personal information and subject to GDPR are disposed within 2 years of contract ending (Client or staff).

S&B CIO is responsible for storing records appropriately and securely on our system.

Paper documents relating to personal information will be shredded.

#### Third party requests

Personal information relating to employees and clients cannot normally be disclosed to an unauthorised third party. These include family members, friends, local authorities, government bodies and the police. There are only certain circumstances when personal information can be given to such third parties and these include:

- prevention or detection of a crime
- apprehension or prosecution of offenders
- prevention of serious harm to a third party
- protection of the vital interests of the data subject, e.g. release of medical data where failure could result in serious harm or death
- ensuring health and safety

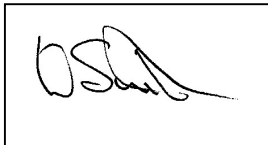
Client and Employees have the right to expect documentary evidence to support such requests.

## **Delivery Plan**

- All IT systems are protected by firewall technology, which is updated regularly, to prevent any “unauthorised access to, or alteration, disclosure or destruction of, the data against their accidental loss or destruction”
- Our bespoke webportal is used by clients to receive data and reports. All information is password protected and held on a secure server
- In addition Smith and Byford have a policy of signing confidentiality agreements with all clients and adhere to any and all specific instructions made by the client regarding any information provided.
- We ensure at all times that we only collect the personal data that is necessary to fulfil the operational needs of any service provided.
- Training is carried out for all staff upon Induction.

## **Review**

The Board of Directors will review the operation of this policy once a year (or more regularly if we identify any non-compliance or problem concerning equality and diversity issues with clients or personnel). We will take remedial action if we discover non-compliance under this policy or barriers to equal opportunities. When reviewing the policy we will consider the outcome of monitoring and review actions under our communications and training plans.



Signed by: Will Smith, Managing Director

Date: June 2018