Health and Safety Policy Statement (BMS02)

This Policy is an Integral Part of our Business covering all of the scope of the Input Group works, including work within the UK Railway Infrastructure.

Appropriate Financial and Physical Resources will be provided to implement this policy.

The Input Group are committed:

- To provide effective control, in so far as reasonably practicable, of the health and safety risks arising from our work activities through compliance with applicable legislation, codes of practice and rail sector requirements including Network Rail, and Railway Group Standards;
- To consult with our employees and subcontractors on matters affecting their health and safety;
- To provide and maintain safe work equipment;
- To ensure safe handling and use of substances;
- To provide information, instruction and supervision for employees and those working on behalf of The Input Group;
- To ensure all employees and those working on behalf of The Input Group are competent to do their tasks, and where necessary to give them appropriate training and support;
- To prevent accidents, incidents and cases of work-related ill health;
- To review all tasks to identify hazards, assess risks and implement effective control measures
- To maintain safe and healthy working conditions;
- To continually improve health and safety performance through the setting of objectives, and monitoring and auditing arrangements;
- To review and revise this policy and arrangements as necessary at regular intervals

Contents of this statement will apply to all areas of the company's business, including those persons working on behalf of the Company, visitors and members of the public interfacing with our activities.

Health & Safety Policy Statement authorised by:

Signed 

Date 3rd June 2018

Quality Policy Statement
(BMS03)

The Input Group provides design, construction, refurbishment and maintenance services for the rail industry and other sectors and the design, manufacture and installation of commercial signage. Our core business is to offer a tailored package of services to fulfil specific project requirements.

The Input Group have a flexible approach, a ‘can do’ attitude and understand commercial expectations. We are committed to work with suppliers and customers to establish and maintain the highest quality standards. Teams are specially selected for each job and we find solutions and implement them in a cost effective and practical way to ensure client satisfaction.

The Input Group is customer focused and delivers its projects through partnership with approved sub contractors and close relationships with its clients.

The Company is committed to continually improve the operation and effectiveness of our ISO 9001 certified quality management system through setting and monitoring quality objectives, compliance with regulatory, Network Rail, Railway Group Standards and construction sector requirements and best practice, and also through identifying and achieving the client’s needs and aspirations.

The content of this Policy will be communicated and explained to employees and to other personnel that may have an influence on the Quality of our Services.

This Quality Policy Statement is authorised by:

Signed 

Date 3rd June 2018

Environmental Policy Statement (BMS04)

The Input Group recognises its design, manufacturing, refurbishment and construction responsibilities and is committed to minimising the impact of its activities on the local and global environment and preventing pollution through a process of continual improvement in its environmental performance.

The key points of its strategy to achieve this are:

- To analyse accepted manufacturing and construction industry solutions, to design-out inefficient, environmentally harmful and wasteful working practices, and to design-in sustainable, economically viable and renewable alternatives wherever possible.
- To minimise waste by evaluating our operations and ensuring that they are as efficient as possible.
- Minimise CO_2 emissions through the careful selection and use of transport, carriage and the source of power requirements and processes.
- Actively promote recycling both internally, on site and amongst its customers and suppliers.
- The disposal of paints, solvents, electronic equipment and other harmful substances and hazardous wastes will be in compliance with legislation, best practice and industry relevant standards.
- Ensure that any discharges from site operations are controlled in accordance with legislative requirements, best practice and relevant consents.
- To source and promote products, equipment and processes to minimise the environmental impact through its lifecycle of manufacture, operation and disposal.
- Meet, or exceed compliance with applicable legislation, codes of practice and rail sector requirements including Network Rail and Railway Group Standards and other requirements that relate to company activities.
- To continue to be compliant with the requirements of our certified ISO14001 integrated Business Management System.

Progress towards achievement of policy requirements will be driven through development of supporting environmental objectives and development of our business processes.

The content of this policy will be communicated and explained to employees and to other personnel that may have an influence on our environmental performance.

Policy Statement authorised by:

Signed 

Date 3rd June 2018

Drugs & Alcohol Policy (BMS05)

As a responsible employer, The Input Group recognise the detrimental effect that drugs and alcohol can have upon an individuals' capability to perform their company responsibilities as defined in their job specifications or contracts and also the harm that drug or alcohol dependency can have on the individual concerned and their families. As we undertake activities on our client's premises, all employees and subcontractors have a duty to comply with their policies with regards to drugs and alcohol. Rail client policies (as defined by Railway Group Standard RIS-8070-TOM and Network Rail Standard NR/L2/OHS/00120) are rigorously enforced and blood alcohol levels of above **29mg/100ml**, 13mgs/100ml of breath or 39mg/100ml of urine will result in an individual being **ejected and banned from site**. (Note this is significantly less than the legal drink-driving limit of **80mg/100ml (of blood)** for England and Wales and **50mg/100ml** of blood in Scotland).

Employee Duties
The Company expects the following **cooperation** from its staff and subcontractors:

- Employees and subcontractors must **not** present themselves for work under the **influence** of alcohol or drugs so that their performance or ability to carry out their activities at work safely and competently is impaired in any way.

- Consumption of alcohol or drugs during normal working hours or at any time on Company or Client premises is prohibited. All workers should also be aware that the body breaks down alcohol at different rates depending on a range of physiological factors and **could be present in the bloodstream the day following its consumption**.

- This Policy covers those **driving** any vehicle on behalf of The Input Group in any capacity or at any location. This Policy covers travel to and from work if it could reasonably be implied that alcohol or drugs were present outside the prescribed limits during normal working hours.

- Employees have a duty to advise their pharmacist/general practitioner of this Policy when being prescribed medication. On their advice, the employee must **notify** his or her manager about any possible impact on his/her health and safety relating to his/her duties at work, so that current or alternative employment can be considered whilst he/she is being prescribed medication. Any employee engaged on safety critical tasks such as electrical works, might require to be provided with alternative work during the period of medical treatment. Subcontractors must complete a Medical Notification Form in the event that they are taking medicines, prior to starting at site.

- Employees and subcontractors obtaining treatment or medicines for themselves should be aware of the conditions and side effects notified and seek out alternatives that do not impair performance through drowsiness or other symptoms. If in doubt consult your Doctor.

Alcohol and Drugs Testing
Employees and subcontractors need to be aware that the Company (and / or the client) may **test** for the presence of alcohol and drugs in the following circumstances:

- Pre-appointment – prior to safety critical workers being authorised through the Sentinel scheme to be able to work lineside they must pass a test and medical.

- 'for cause' – meaning there are reasonable grounds to believe that the influence of drugs and/or alcohol has lead or had to the potential to lead to an unsafe situation, or abnormal behaviours.

- Random testing – sampling will be based upon the level of risk associated with job functions with a target of a 5% sample.

  (Note: refusal to undertake testing for D&A will be treated as a failure i.e. a positive test)

Company Duties

This policy is not a means to victimise individual employees but to ensure that the Input Group can meet its legal obligations and client expectations whilst being able to consider its duty to its employees.

Breaching of this policy will result in the individual being notified of a positive result and suspended from duty pending an inquiry. For any relevant staff holding Sentinel competence, the Sentinel database will be updated and their Sentinel card withdrawn.

Individuals identified as breaching this policy will be managed depending upon the circumstances associated with the **breach**. In general, the two main courses of action will be either:

- Disciplinary action in accordance with company procedures (and the Sentinel Scheme Rules if applicable).

- Company management will provide guidance to employees in seeking professional support if alcohol or drug dependency issues are identified.

This Policy Statement is authorised by:

Signed 

Date 3rd June 2018

Equality & Diversity Policy Statement (BMS06)

The Input Group offers a non-discriminatory environment in employment to all staff and applicants. We support the principal of equal opportunities in employment to ensure that the talents and resources of employees are fully utilised and that no job applicant or employee receives less favourable treatment on the ground of:

- Gender (including marital status, sexual orientation & pregnancy);
- Age
- Social standing;
- Race & ethnic origin;
- Religion & religious belief;
- Disability;
- Convictions spent under the Rehabilitation of Offenders Act.

This policy includes the commitment to maintain a working environment free from sexual harassment.

The Company Director has ultimate responsibility for equality and diversity matters within the organisation. Management are responsible for monitoring the effectiveness of the policy, assessing the policy objectives and proposing procedural improvements where necessary.

All employees have a responsibility to accept their personal involvement in the practical application of this policy but specific responsibility falls upon staff involved in recruitment, employee administration and training.

This policy applies to all terms, conditions and privileges of employment including; recruitment, hiring, probationary periods, training and development, job assignments, supervision, promotion, rates of pay or benefits, transfer, educational assistance, layoff and recall, terminations and retirement.

Each manager and supervisor is responsible to ensure the consistent interpretation of this policy.

Employees should normally bring any work-related complaints under the policy to their supervisors as with other employee complaints. Every effort will be made to treat complaints promptly, impartially and confidentially with a view to arriving at fair resolutions.

We will provide, upon request by the applicant reasonable accommodations for the employees disability when doing so will enable him or her to successfully perform the essential duties of the job.

To this end The Input Group will:

- Recognise its legal obligations to job applicants and employees and endeavour to fulfil its social responsibility to such individuals;
- Review periodically its selection criteria and procedures to maintain a system where individuals are selected, promoted and treated solely on the basis of their merits and abilities which were appropriate to the job;
- Distribute and publicise this policy throughout the organisation and elsewhere as is from time to time appropriate, and will ensure that all staff are notified of any amendments to the policy;
- Ensure that staff responsible for recruitment, selection, promotion, interviewing, grievance and disciplinary matters are made aware of how the policy is to be implemented and their position in the law. Training will be provided where necessary;
- Provide facilities for any employee who believes that inequitable treatment has been applied to him or her within the scope of this policy to raise the matter through the appropriate grievance procedure as detailed in the staff handbook, maintained in the company's BMS and is also published in site files;
- Ensure that it is aware of the make-up of the current workforce and applicants and determine whether this demonstrates equal opportunity.

Breaches of this policy by employees will be treated as a disciplinary offence and will be dealt with, as for any other breach of the organisations policies, under the internal disciplinary procedure.

This policy and its implementation will be reviewed on a regular basis with changes in relevant legislation or at least annually.

This Policy Statement is authorised by:

Signed 

Date 3rd June 2018

Workplace Bullying & Harassment Policy (BMS07)

The Input Group is committed to preventing harassment and bullying and creating a culture at in which harassment and bullying cannot flourish. The recipient of perceived harassment and bullying could make claims on the grounds of race/ethnicity, sex / gender, age, disability or religious intolerance.

Employees must ensure that through their actions, there are no grounds for allegations of such behaviour that can be made by work colleagues, or representatives of clients, subcontractors, suppliers and the public.

Through the induction process, internal communication and appraisal system, the Company will make employees aware of accepted behaviours within the business environment. Individuals should treat others in the manner that they would expect to be treated themselves.

Allegations of harassment and bullying received either formally or informally through this policy must be taken seriously by managers and dealt with promptly and sensitively.

Employees who are aware of potential situations that may lead to allegations of bullying or harassment should make their line manager aware of the circumstances.

Where it is possible to resolve the matter by informal means, every effort should be made to do so.

Where a complaint of harassment and bullying is upheld, this could result in disciplinary action being taken against the perpetrator. The Company views harassment and bullying as unacceptable behaviours.

The Company will ensure that any member of staff raising a concern under this policy is not victimised as a result.

This Policy Statement is authorised by:

Signed 

Date 3rd June 2018

Work Safe Policy (BMS08)

The Input Group is committed to providing employees and subcontractors working on our behalf with a safe working environment and systems of work. We have a moral and statutory responsibility to ensure the health, safety and well-being of our workforce, and the protection of the environment.

The principle of this Work Safe (or Refusal to Work) Policy is to empower personnel under the Company's control to refuse to work in conditions, or undertake working practices that they reasonably consider to be hazardous.

Safe systems of work - in order to plan for a safe working environment, The Input Group will risk assess all activities and implement and communicate suitable and sufficient control measures. It is the responsibility (under the Health and Safety at Work Act 1974) of all personnel working on our sites and in our offices to report deficiencies in these arrangements to our management immediately.

Competent workforce - employees and subcontractors are expected that they will only undertake work in which they have been trained, deemed competent and authorised to do so. The scope of works will be discussed through site induction, and the workforce liaising with supervisors to assess changes to activities.

Safe and suitable behaviours – employees and subcontractors have a duty to adhere to client and Input Group policies and arrangements. Duties include following site rules, applying to control measures identified in risk assessments and method statements, wearing specified PPE and utilising suitable tools and equipment.

Individuals (or groups) must report immediately to site management / supervision if they refuse to work on the grounds of health, safety or environmental risk concerns, including instances of fatigue for safety critical workers. Such instances shall be reported as a **Close Call** by the worker(s) concerned and resolved by the person it was reported to. If the issue cannot be resolved locally, then it must be reported to Input Group Management for them to find a solution. If individuals concerns are not being addressed, it can be reported to the **Confidential Incident Reporting & Analysis System** www.ciras.org.uk. Personnel reporting reasonable concerns will not be unfairly treated or penalised for doing so.

The Company are members of the CIRAS scheme. The company's General Manager has been appointed as the company's CIRAS representative to be the single point of contact for receiving reports and is also responsible for responding to issues/reports received. The Company's CIRAS representative is also responsible for ensuring the distribution of the CIRAS Newsletter is carried out and that the communication of CIRAS messages are undertaken as required through tool-box talks and /or written briefings as appropriate.

This Policy Statement is authorised by:

Signed 

Date 3rd June 2018

Anti-Bribery and Corruption Policy (BMS09)

The Input Group values its reputation for ethical behaviour and integrity. Conducting business with a zero tolerance approach to all forms of corruption is central to these values, the Company's image and reputation. This policy below sets out the standards expected of all employees in relation to anti-bribery and corruption. In particular, all employees must adhere strictly to relevant laws in this area, in particular The Bribery Act 2010.

The Policy is also relevant for other interested parties who perform services for or on behalf of the Company. The Input Group expects those persons to adhere to the Policy or have in place equivalent policies and procedures to combat bribery and corruption.

The Company will ensure any concerns are investigated appropriately and any employee making a report in good faith shall suffer no detriment for doing so. The Company will take firm action against any individuals or other parties that it discovers are involved in bribery. Any breach of the Policy by employees will result in disciplinary action under the Company's procedures.

Failure by any employee to report corrupt activity by other persons can also result in disciplinary sanctions, especially where there is evidence that an employee has attempted to cover up or disguise another's wrongdoing.

The Input Group has a zero-tolerance policy towards corruption of all kinds.

Employees should note that it is a criminal offence to offer, promise, pay, request or accept a bribe.

A bribe does not need to be a monetary sum. It can be any form of advantage, offered or received.

A contract does not need to have been won for a corruption offence to have been committed.

The Policy consists of four main rules that all employees must adhere strictly to:

- Do not offer, promise or pay bribes.
- Do not request, agree to or accept bribes.
- Do not make payments to someone (or favour then in any other way) if you know that this will involve someone in misuse of their position (or them performing their functions improperly).
- Do not misuse your position (or perform your functions improperly) in connection with payments (or other favours) for yourself or others.

Reasonable and Proportionate Gifts and Hospitality

This Policy is not meant to prohibit the giving or receiving of reasonable and proportionate gifts and hospitality as long as they are appropriate in all the circumstances and there is no risk or perception that they might improperly influence the recipient.

They do not contravene any rules applying to the individual to whom the hospitality or gift is offered (i.e. any policy that another organisation has in place) or any laws applying to that other person.

The expenditure in question is not related to some actual or anticipated business with the recipient, particularly in a competitive context.

In the case of hospitality provided or received intended to foster cordial relations, it has to have legitimate marketing purposes and the level of hospitality is appropriate with regard to the recipient and their organisation and must never be cash.

All Sponsorship and donations made on behalf of the Company must be approved in advance by the Company Owner.

Anti-Bribery and Corruption Policy (BMS09)

Facilitation (small unofficial) payments to speed up administrative processes, are bribes and prohibited by this Policy. Where an employee suspects a demand for a payment is a request for a facilitation payment, this must be reported immediately to the Company Owner.

Employees must read, understand and comply with this Policy.

The Company Owner has overall responsibility for ensuring this Policy complies with the Company's legal and ethical obligations and to ensure everyone in The Input Group complies with it.

Management at all levels are responsible for ensuring those reporting to them are made aware of and understand this Policy.

This Policy Statement is authorised by:

Signed 

Date : 3rd June 2018

ENERGY MANAGEMENT POLICY (BMS10)

The Input Group's corporate mission is to provide:

- The best possible facilities and highest level of customer service providing building information modelling to our clients.
- A rewarding work environment to our employees

In pursuit of this mission, The Input Group will strive to achieve a nationwide reputation for energy management. We are committed to a high performance portfolio that uses energy in the most efficient, cost-effective, and environmentally responsible manner possible.

Energy management will play a key role in our business. It will support our plan to maximize profitability, strengthen our competitive position, and provide clients with the highest quality of services. Our efforts to reduce energy use and prevent pollution will also support our commitment to our employees, the environment, and the communities in which we are a part.

Toward this end, The Input Group shall work towards continuously improving energy performance. We will establish specific implementation plans by 30/11/14, and will have made significant achievements in this area within 5 years' time.

The Input Group's objectives as related to this policy are the following:

- Provide the best possible environment for occupants of facilities created by ourselves, while simultaneously maximizing energy performance
- Reduce operating expenses and increase asset values by actively and responsibly making provision for managing energy consumption
- Demonstrate commitment to our community and leadership in the construction industry, by reducing pollution associated with energy use

The Input Group will endeavour to meet or exceed the following energy management targets in service to these objectives:

- Reduce energy consumption in existing buildings by 25% over a 5-year period
- Reduce energy intensity (kBtu/sf) by 25% in existing buildings over a 5-year period
- Design and construct all new developments to achieve 30% energy savings over local building energy codes
- Reduce carbon emissions associated with energy consumption by25% by 2020

This policy shall apply to all of The Input Group's properties, business units, employees, and contractors in service to our portfolio.

This Energy Management Policy Statement is authorised by:

Signed 

Date……30th June 2017…….

Training/Staff Development Policy Statement (BMS11)

Sufficient and appropriate training to underpin competence of personnel is the key to the efficient operation of the company. The company does not see training as an activity undertaken just to meet the minimum requirements of health and safety law and sector requirements. Neither does it see health and safety training as a 'bolt-on' extra to skill or professional training, but as an integrated part of general skill training, for the correct undertaking of any work activity.

The nature of the company's activities requires high levels of competence for personnel undertaking high-risk work. This will be developed through identifying training needs, assessing performance and reviewing knowledge. Competence requirements are defined within role Job Descriptions. The purpose of this policy and associated procedures is to develop personnel through training and assessment. A Competency Management procedure defines the process for development and approval of personnel working in a rail trackside environment.

The company has therefore set out its aims to training as follows:

1. Training that is both suitable and sufficient and cost effective.
The degree of risk to be countered by the training will be taken into account when deciding if the training is justified.

2. Training will be prioritised to ensure that training, information and instruction for high-risk activities and emergency procedures is undertaken before general skill training.
The company objective is to ensure that all employees can carry out their duties with the least chance of harm occurring either to themselves or to others; or causing damage to property.

3. The more information, instruction and training received by the employee, the greater their level of competence and therefore the greater the opportunity to act as supervisors of their own work.
The company will maintain records of all training and regular reviews of training needs are undertaken from which a training plan can be developed.

All new starters with the company will undergo induction training to make them aware of the Company's Policies and Business Management Systems, its structure and requirements.

All employees will be given on site instruction as to site requirements applicable to each site and undergo a client / principal contractor site induction.

Staff Development
The company's mission is to enhance the current and future organisation effectiveness by increasing its employee's abilities to maximise performance. The company is committed to supporting the continual growth and development of its most valuable assets, its people.

The Input Group underpins this policy by:

- Cultivating its workforce and enhancing the company's culture through professional development programs.
- Promoting diversity to protect individuals from discrimination and harassment (see Equality & Diversity Policy (BMS06) & Workplace Bullying & Harassment Policy (BMS07).
- Assisting individuals in developing their interpersonal and managerial skills.
- Improving the quality of work life, job satisfaction and motivation for employees. Resulting in the retention of an effective workforce.
- Educating employees so they can best utilise the benefits, services, policies and procedures of the Input Group.

This Policy Statement is authorised by:

Signed 

Date: 3rd June 2018

Management of Fatigue and Working Hours Policy (BMS12)

The Input Group has a duty to ensure that all personnel involved in work carried out on Network Rail Infrastructure are not subjected to fatigue through excessive hours of work, as part of our compliance with The Railways and Other Guided Transport Systems (Safety) Regulations 2006 (ROGS) and Network Rail Standard NR/L2/ERG/003 'Management of Fatigue: Control of Excessive Working Hours for Persons Undertaking Safety Critical Work'. The Input Group is responsible for setting up a system to monitor excessive working hours and fatigue, and responsible for briefing all information regarding working hours to all of our employees, sub-contractors and Agency staff as applicable.

It is The Input Group's policy, and in line with Network Rail requirements that personnel should only work:

- A max. of 12 hours per shift on site (max 14 hours with travelling time)
- A max. of 72 hours per week worked on site
- A min. of 12 hours rest period between shifts on site
- A maximum of 13 shifts out of a possible 14 shifts in any two-week cycle.
- There are exceptional circumstances where these rules may be breached. This may include essential emergency engineering works that may affect operational safety and mass disruption to Network Rail Infrastructure.
- Planned engineering works that have over run, and it is not reasonably practical to make alternative arrangements.
- Providing emergency services in the case of an incident or fatal accident regarding Passengers or other Infrastructure users i.e. other contractors or Train Operating Companies.

Authority to exceed working hours
Any breach of this Company Policy must be agreed in writing by the Company and the Client's representative.

A risk assessment must be completed before any excessive work takes place. The assessment must identify the hazards associated with fatigue and record the control measures to be implemented.

This Policy Statement is authorised by:

Signed 

Date: 3rd June 2018

Sustainability Policy Statement
(BMS13)

The Input Group is committed to promoting sustainability. We recognise that all firms and individuals have an important role to play in reducing negative environmental impacts and specifically tackling climate change. As such, concern for the environment and the promotion of a broader sustainability agenda are integral to The Input Group's activities and the management of the organisation. We aim to follow and to promote good sustainability practice, to reduce the environmental impacts of all our activities and to help our clients and partners to do the same.

We have developed the Input Group Sustainability Policy, which comprises a set of principles, operating procedures and business targets.

Principles

Our Sustainability Policy is based upon the following principles:

- To comply with, and exceed where practicable, all applicable legislation, regulations and codes of practice.
- To integrate, where practicable, sustainability considerations into all our business decisions.
- To ensure that all staff are fully aware of our Sustainability Policy and are committed to implementing and improving it.
- To minimise the impact on sustainability of our premises and transportation activities.
- To make clients and suppliers aware of our Sustainability Policy, and encourage them to adopt sound sustainable management practices.
- To review, annually report, and to continually strive to improve our sustainability performance.

In order to put these principles into action and to reduce our negative environmental impacts as a firm and as individuals, The Input Group implements the following procedures:

Minimising carbon emissions from travel

- Where possible, employees should use public transport, walk or cycle to attend meetings, apart from in exceptional circumstances where this is impractical and/or cost prohibitive.
- Wherever possible, employees use clean-tech vehicles rather than traditionally powered cars and aircraft
- All employee air travel requires Director sign-off and is subject to review to determine if alternative travel arrangements have been explored.
- Wherever possible and practicable, employee travel within the UK, will be undertaken by train
- The Input Group shall provide employees with technology options that provide an alternative that can avoid the need to physically travel to meetings, including teleconferencing, web cams, and the efficient timing of meetings to avoid multiple trips.
- The Input Group will reduce the need for our staff to travel by supporting alternative working arrangements, including home working
- The Input Group will promote the use of public transport by locating our offices in accessible locations.

Minimise water consumption, waste & maximise recycling

- The Input Group believes that the consumption of bottled water in an office or hospitality context is unnecessary. We use mains water in our office environment and request that venues to do the same for all The Input Group events and meetings.

- Minimise our use of paper and other office consumables, for example by double-siding "duplexing" all paper used where practicable.
- As far as possible arrange for the reuse or recycling of all waste, including paper, computer supplies and redundant equipment.
- Reduce the energy consumption of office equipment by purchasing energy efficient equipment and employing good housekeeping (switching off equipment that is not in use).

Working practices

- The Input Group seeks to build and deliver its sustainability solutions on the most resource efficient computing platform.
- The Input Group undertakes regular annual employee awareness sessions to ensure every employee adheres to our sustainability policy
- Wherever possible we source products and services from suppliers with a sustainability policy. This primarily covers printing supplies, stationery, computing equipment and business travel.
- The Input Group requests that every employee takes account of sustainability issues in their advice to clients.
- The Input Group will include a copy of our Sustainability Policy in all our proposals to clients.

Reporting our progress

- The Input Group will use its own sustainability and emissions management solution to monitor our impact in real-time and identify potential sustainability opportunities.
- The Input Group will report annually our environmental impact and progress against sustainability goals.

The Input Group Sustainability Targets

- Reduce water consumption from the company's Head Office per employee by 10% by 2019 against a 2014 baseline
- To reduce the demand for non-sustainable goods and services by procuring resource efficient products and considering end of life. The company to incorporate whole life costing considerations into construction, refurbishment and maintenance contracts
- To reduce the company's carbon footprint, focusing particular on the reduction in use of gas and electricity from the national grid. Gas an electricity consumption to be reduced by 5% from the 2014 baseline by 2019.

Breaches of this policy by employees will be treated as a disciplinary offence and will be dealt with, as for any other breach of the organisations policies, under the internal disciplinary procedure. This policy and its implementation will be reviewed on a regular basis with changes in relevant legislation and at least annually.

This Policy Statement is authorised by:

Signed 

Date; 3rd June 2018

Ethical and Client Focus Policy Statement (BMS14)

The Input Group operates its business in accordance with a number of general principles, which are set out in this Ethical Conduct Policy.

The purpose of these principles is to support the development of sound and successful business, which respects the needs of users of our projects, employees and other people affected by our activities. In addition, we will endeavor to ensure that our sub-contractors abide by the principles of our Ethical Conduct Policy.

We comply with legal requirements - in bidding for new business and implementing projects once they have been awarded.

Business Ethics

We are committed to carrying out our business with high standards of integrity and ethics: avoiding unfair anticompetitive practices, ensuring that company information is maintained confidentially and securely and avoiding all forms of corruption and bribery. Employees should declare any outside business interests and any conflicts of interest, which may arise. *(See - Anti Bribery and Corruption Policy reference BMS09 for further details*).

Relationship with External Parties and Clients

We will listen and respond to reasonable enquiries raised by external parties who are affected by our activities and will communicate with them in a timely manner.

The Inputgroup believes in full transparency in all its dealings. There are three primary dimensions of company transparency:

- Information
- Disclosure,
- Clarity and accuracy.

To increase transparency, The Input Group believes in developing greater disclosure, clarity, and accuracy into our communications with stakeholders, including the handling of complaints. The Business has a responsibility beyond its basic responsibility to its owners; a responsibility to a broader constituency that includes its key customers, employees, government and the people of the communities in which it operates.

Transparency with clients and suppliers also includes price transparency. Where price savings can be achieved through efficiencies, alternative processes, alternative more long-term cost-effective solutions etc. will be disclosed and shared with the client/supplier.

Anti-Slavery and Human Trafficking

Modern slavery is a term used to encompass slavery, servitude, forced and compulsory labour, bonded and child labour and human trafficking. Victims are coerced, deceived and forced against their free will into providing work or services. Human trafficking is where a person arranges or facilitates the travel of another person with a view to that person being exploited. Modern slavery is a crime and a violation of fundamental human rights.

The Input Group strictly prohibits the use of modern slavery and human trafficking in our operations and supply chain. We are committed to implementing systems and controls aimed at ensuring that modern slavery is not taking place anywhere within our organisation or in any of our supply chains. We expect that our suppliers will hold themselves and their own suppliers to the same high standards.

We expect everyone working with us or on our behalf to support and uphold the following measures to safeguard against modern slavery:

- We have a zero-tolerance approach to modern slavery in our organisation or our supply chains. The prevention, detection and reporting of modern slavery in any part of our organisation or supply chain is the responsibility of all those working for us or on our behalf. Workers must not engage in, facilitate or fail to report any activity that might lead to, or suggest, a breach of this policy.
- We are committed to training relevant employees in modern slavery, how to identify it in practice and how to respond.
- We are committed to engaging with our direct suppliers where possible to address the risk of modern slavery in our operations and supply chain.
- As part of our contracting processes, where we are able to negotiate the terms of supply we negotiate to include a specific prohibition against the use of modern slavery and trafficked labour and an ability to audit the supplier's organisation for compliance with this policy.

Whole Life Costing

Clarity, honesty and accuracy are critical in discussions with clients in Whole Life costing of projects where applicable. The company shall ensure time is set aside to openly discuss with the clients, designers etc. to agree the performance requirements that should be taken into account before the costing exercise is commenced. Whole life costing is relevant when considering whole estates, whole facilities, individual buildings or structures and when comparing alternative scenarios such as: retain, refurbishment, alternative designs and alternative specifications etc.

Benefits of Whole Life Costing include:

- Analysis of business needs and communication of these to the project team.
- Ensuring risk and cost analysis of loss of functional performance due to failure or inadequate maintenance occurs,
- Promoting realistic budgeting for operational maintenance and repair.
- Discussion and recording of decisions about durability of materials and components at the outset of the project.
- Optimising the total cost of ownership occupation by balancing initial capital and running costs,

Supporting the benefits of Whole Life Costing, The Inputgroup works closely with the client to identify improved technology, sustainable products, maintenance reduction systems etc. to produce value added improvements to the client's assets.

Mission

- To deliver superior performance by consistently taking a long-term view and fully integrating sustainability research within a rigorous client focused framework. Delivering outstanding results will also achieve our goal of proving the business case for a sustainable future.
- To create long-term client partnerships by delivering unique services and exceptional client focus.
- To attract, retain and develop the best professionals within a passionate investment culture and with whom we share a commitment to Our Values.

Our Values

Commitment to Clients

We are committed to providing exceptional client service — above all by delivering superior long-term performance — and by ensuring that our interests are fully aligned with those of our clients.

Ethical and Client Focus Policy Statement (BMS14)

Integrity
Integrity and honesty form the bedrock of our business. We expect the highest ethical standards in our work and personal lives.

Excellence and Innovation
We aim for excellence in all that we do, and ensure that our processes encourage rigorous research, curiosity and continuous learning. We believe interdisciplinary, diverse teams are the most likely to yield new insights and produce the best results for our clients over the long-term.

Teamwork
Teamwork underpins our firm culture. We consider each of the women and men with whom we work as individuals entitled to respect and dignity, and we recognise and reward their contributions on the basis of merit.

Communication
Effective communication is critical to teamwork and to our relationships. We encourage and especially value hearing different viewpoints and respectful challenges to consensus opinions.

Diversity
Diversity, in the broadest sense, helps drive our success. A welcoming work environment, where individuals can bring the totality of their experience and perspectives, is an invaluable contributor to greater economic success.

Independence
We have chosen an independent broad-based owned partnership as an enduring business model. Similarly, we are committed to remaining a family firm focused on continual improvement in our performance.

Responsible Citizenship
We recognise and accept our responsibility to live in accordance with our values, to be responsible to the communities in which we live and work and to the broader community. We aim to reduce our environmental footprint where possible, we are mindful of ways to help our employees fulfill their personal responsibilities, and we actively encourage engagement with local voluntary organisations.

Employment Practices
We maintain a working environment where all employees are treated with dignity and respect. We are committed to providing equal opportunities for all employees regardless of their race, colour, ethnic origin, religious belief, sexual orientation, marital status, age, nationality or disability. We are committed to engaging in open communication with our employees

Risk Mitigation
Mitigation of risk is a part of the discipline of risk management. Mitigation plans eliminate the exposure of a business to risk, lessen the impact of a threat, or reduce the frequency or severity of risks. In order for mitigation to be effective, the risks must be identified ahead of time and a plan devised ready for implementation before or when the risk occurs. The plan itself depends on the type and level of risk the business faces. Business risks commonly fall within one of four areas: strategic, compliance, financial or operational risks.

To this end the company have produced a robust Business Continuity Plan that has identified the potential risks and treats to business and the desired mitigation actions to reduce the identified risks to acceptable levels to ensure that the company can continue to provide its clients with a continuity of service.

This Policy Statement is authorised by:

Signed 

Date: 3rd June 2018

Information Security Policy

(BMS15)

VERSION HISTORY

Version	Date Issued	Brief Summary of Change	Owner's Name
Draft	01/02/2016	Draft Issue	Adrian Monk
1.0	02/02/2016	For implementation	Adrian Monk
2.0	30/04/2018	Amended following review of the GDPR	Adrian Monk

Policy title:	**Information Security Policy**

Aim:	The aim of this policy is to establish and maintain the security and confidentiality of information, information systems, applications and networks owned or held by The Inputgroup.

Scope:	This policy applies to all information, information systems, networks, applications, locations and users of The Inputgroup or supplied under contract to it

Associated documentation:	**Legal Framework:** General Data Protection Regulations (2018) The Data Protection Act (1998), Copyright Designs & Patents Act (1988), Computer Misuse Act (1990) Amendment Act, (2005) Health & Safety at Work Act (1974), Human Rights Act (1998) **Policies:** Disciplinary Policy and Procedure (EMP02) Grievance Procedure (EMP03) Business Continuity Plan
Appendices:	Appendix 'A' – Principles of the General Data Protection Regs 2018 Appendix 'B' - A summary of the Data Protection Act 1998
Approved by:	Adrian Monk (Owner/Director, The Inputgroup.)
Date:	30/04/2018

Review and consultation process:	Annually from review date above.
Responsibility for Implementation & Training:	Brian Lomas (Information Compliance Manager)

-

Introduction

This top-level information security policy is a key component of the Inputgroup overall information security management framework and should be considered alongside more detailed information security documentation including, system level security policies, security guidance and protocols or procedures.

Objectives, Aim and Scope

2.1. Objectives

The objectives of The Inputgroup Information Security Policy are to preserve:

- **Confidentiality** - Access to Data shall be confined to those with appropriate authority.
- **Integrity** – Information shall be complete and accurate. All systems, assets and networks shall operate correctly, according to specification.
- **Availability** - Information shall be available and delivered to the right person, at the time when it is needed.

2.2. Policy aim

The aim of this policy is to establish and maintain the security and confidentiality of information, information systems, applications and networks owned or held by The Inputgroup by:

- Ensuring that all members of staff are aware of and fully comply with the relevant legislation as described in this and other policies.
- Describing the principals of security and explaining how they shall be implemented in the organisation.
- Introducing a consistent approach to security, ensuring that all members of staff fully understand their own responsibilities.
- Creating and maintaining within the organisation a level of awareness of the need for Information Security as an integral part of the day to day business.
- Protecting information assets under the control of the organisation.

2.3. Scope

This policy applies to all information, information systems, networks, applications, locations and users of The Inputgroup or supplied under contract to it.

2.4. Responsibilities for Information Security

2.5. Ultimate responsibility for information security rests with the Owner/Director of The Inputgroup, but on a day-to-day basis the

Information Governance Compliance Manager shall be responsible for managing and implementing the policy and related procedures.

2.6. Line Managers are responsible for ensuring that their permanent and temporary staff and contractors are aware of: -

- The information security policies applicable in their work areas
- Their personal responsibilities for information security
- How to access advice on information security matters

2.3. All staff shall comply with information security procedures including the maintenance of data confidentiality and data integrity. Failure to do so may result in disciplinary action.

2.4. The Information Security Policy shall be maintained, reviewed and updated during the Annual Management Review process or following any legislation change/attempted security breach.

2.5. Line managers shall be individually responsible for the security of their physical environments where information is processed or stored.

2.6. Each member of staff shall be responsible for the operational security of the information systems they use.

2.7. Each system user shall comply with the security requirements that are currently in force, and shall also ensure that the confidentiality, integrity and availability of the information they use is maintained to the highest standard.

2.8. Contracts with external contractors that allow access to the organisation's information systems shall be in operation before access is allowed. These contracts shall ensure that the staff or sub-contractors of the external organisation shall comply with all appropriate security policies.

Legislation

3.1. The Inputgroup is obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation shall be devolved to employees and agents of The Inputgroup, who may be held personally accountable for any breaches of information security for which they may be held responsible. The Inputgroup shall comply with the following legislation and other legislation as appropriate:

- The General Data Protection Act (GDPR) (2018)
- The Data Protection (Processing of Sensitive Personal Data) Order 2000.
- The Copyright, Designs and Patents Act (1988)
- The Computer Misuse Act (1990) Amendment Act, (2005)
- The Health and Safety at Work Act (1974)
- Human Rights Act (1998)
- Regulation of Investigatory Powers Act 2000
- Freedom of Information Act 2000

- Health & Social Care Act 2001

5. Policy Framework

5.1. Management of Security

- At board level, responsibility for Information Security shall reside with the Owner/Director.
- The Inputgroup Head of Information Compliance shall be responsible for implementing, monitoring, documenting and communicating security requirements for the organisation.

5.2. Information Security Awareness Training

- Information security awareness training shall be included in the staff induction process.
- An ongoing awareness programme shall be established and maintained in order to ensure that staff awareness is refreshed and updated as necessary.

5.3. Contracts of Employment

- Staff security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain a confidentiality clause.
- Information security expectations of staff shall be included within appropriate job definitions.

5.4. Security Control of Assets

Each IT asset, (hardware, software, application or data) shall have a named custodian who shall be responsible for the information security of that asset. The Inputgroup operates an intranet system that's server is not directly connected to the internet. Access to the internet is managed through boundary security devices such as firewalls etc. and access is restricted to authorised personnel only by the Head of Information Compliance. Any security patches released by software/OS suppliers are managed through periodic maintenance processes under the supervision of the Head of Information Compliance

5.5. Access Controls

Only authorised personnel who have a justified and approved business need shall be given access to restricted areas containing information systems or stored data.

5.6. User Access Controls

Access to information shall be restricted to authorised users who have a bona-fide business need to access the information.

5.7. Computer Access Control

Access to computer facilities shall be restricted to authorised users who have business need to use the facilities.

5.8. Application Access Control

Access to data, system utilities and program source libraries shall be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators. Authorisation to use an application shall depend on the availability of a licence from the supplier.

5.9. Equipment Security

In order to minimise loss of, or damage to, all assets, equipment shall be physically protected from threats and environmental hazards.

Equipment Disposal

All IT equipment for disposal must have Hard disks or other storage media removed first.

All storage media must be disposed of securely either by physical destruction or through a government approved disposal company.

Records of such media must be kept.

Bring your Own Device

Employees or Sub-contractors can use their own IT equipment subject to the following.

Permission from the General Manager & Risk assessment

Equipment must have a supported operating system & be up to date.

Equipment must have Paid for Anti-Virus software that is fully functional and approved

Any Company Data stored on this device must be protected from loss by means of password / encryption.

If required as part of any investigation the company reserves the right to inspect the equipment.

Any software/services installed that are licensed to the company will be removed once the device is no longer used or needed.

Mobile Phones

Company supplied mobile phones will be kept up to date with the latest security updates.

Mobile Phones will have PIN or passcode protection enabled

Android based Phones must have Anti-Virus software installed.

End of life Mobile phones must be destroyed or wiped securely.

5.10. Computer and Network Procedures

Management of computers and networks shall be controlled through standard documented procedures that have been authorised by the Owner/Director.

5.11. Information Risk Assessment

Once identified, information security risks shall be managed on a formal basis. They shall be recorded within a baseline risk register and action plans shall be put in place to effectively manage those risks. The risk register and all associated actions shall be reviewed at regular intervals. Any implemented information security arrangements shall also be a regularly reviewed feature of The Inputgroup's risk management programme. These reviews shall help identify areas of continuing best practice and possible weakness, as well as potential risks that may have arisen since the last review was completed.

5.12. External Shared Data

Any shared data from external sources such as clients, suppliers or contractors etc. shall be subject to a robust risk assessment to ensure security of all party's data. All significant risks and mitigations that have implications for security of clients, suppliers or contractors etc. information assets shall be reviewed by all parties and a joint plan shall be agreed prior to any contract being started. Any Inputgroup staff/contractor that may have a significant role in contractual activities associated with client information security systems may be subject to DBS (Disclosure and Barring Service) checks prior to appointment.

5.13. Information security events and weaknesses

All information security events and suspected weaknesses are to be reported to the

General Manager
Telephone 01332 348830 (ext. 24)
Mobile 07801926218
Email k.smith@inputgroup.co.uk

All information security events shall be investigated to establish their cause and impacts with a view to avoiding similar events.

5.14. Protection from Malicious Software

The organisation shall use software countermeasures and management procedures to protect itself against the threat of malicious software. All staff shall be expected to co-operate fully with this policy. Users shall not install software on the organisation's property without permission from the Information Governance Compliance Manager. Users breaching this requirement may be subject to disciplinary action.

5.15. User media

Removable media of all types that contain software or data from external sources, or that have been used on external equipment, require the approval of Information Governance Compliance Manager

before they may be used on the Inputgroup's systems. Such media must also be fully virus checked before being used on the organisation's equipment. Users breaching this requirement may be subject to disciplinary action.

5.16. Monitoring System Access and Use

An audit trail of system access and data use by staff shall be maintained and reviewed on a regular basis.

The organisation has in place routines to regularly audit compliance with this and other policies. In addition, it reserves the right monitor activity where it suspects that there has been a breach of policy. The Regulation of Investigatory Powers Act (2000) permits monitoring and recording of employees' electronic communications (including telephone communications) for the following reasons:

- Establishing the existence of facts
- Investigating or detecting unauthorised use of the system
- Preventing or detecting crime
- Ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system (quality control and training)
- In the interests of national security
- Ascertaining compliance with regulatory or self-regulatory practices or procedures
- Ensuring the effective operation of the system.

Any monitoring will be undertaken in accordance with the above act and the Human Rights Act

5.17. Accreditation of Information Systems

The organisation shall ensure that all new information systems, applications and networks include a security plan and are approved by the Owner/Director of the Inputgroup, before they commence operation.

5.18. System Change Control

Changes to information systems, applications or networks shall be reviewed and approved by the Information Governance Compliance Manager.

5.19. Intellectual Property Rights

The organisation shall ensure that all information products are properly licensed and approved by the Information Governance Compliance Manager. Users shall not install software on the organisation's property without permission from the Information Governance Compliance Manager. Users breaching this requirement may be subject to disciplinary action.

5.20. Business Continuity and Disaster Recovery Plans

The organisation shall ensure that business impact assessment, business continuity and disaster recovery plans are produced for all mission critical information, applications, systems and networks.

5.21. Reporting

The Information Security Officer shall keep the Owner/Director of the Input Group informed of the information security status of the organisation by means of regular reports and presentations.

5.22. Policy Audit

This policy shall be subject to audit by Business Management System (BMS) Advisor as part of the internal audit process.

6.0 Personal Data Protection

The Input Group complies with the protection of personal data as stated within the requirements of the General Data Protection Regulations. Personal data is processed in accordance with the six data protection principles;

1. Processed lawfully, fairly and transparently.
2. Collected only for specific legitimate purposes.
3. Adequate, relevant and limited to what is necessary.
4. Be accurate and kept up to date.
5. Data to be stored only as long as necessary.
6. Ensure appropriate security, integrity and confidentiality.

6.1 Data Processing

Due to the nature of The Input Group's activities, the processing of personal data is very limited and is only processed for the most appropriate and legitimate interests. Data will be limited to;

a. Paybills/HMRC legal required data.
b. Training/Competence data.

Paybills/HMRC data comprises of;

a. Full name
b. Address
c. NI number
d. Contact details
e. Company Pay-bill number
f. UTR (Unique Taxpayer Reference) number
g. VAT Registration number (if applicable)

Such data is processed utilising the HMRC approved software (Sage). Access to the Sage software is fully controlled and only personnel within the accounts department and the company's General Manager has access to process and view the data.

Training/Competence Data.

Training and competence data is held within the company's Business Management System comprising of a Microsoft excel spreadsheet that identifies appropriate qualifications, training required, training undertaken with expiry dates as applicable. Electronic held data also includes copies of curriculum vitae (CV), industry held ID cards i.e. PASMA, CSCS, CPCS etc. as appropriate to employment with the company. Only the company's BMS Advisor and the General Manager has access to amend and update the data as applicable. The data is used to identify personnel with the correct competence to be allocated to tasks relevant to their qualifications and experience by the General Manager.

No Special Category of Personal Data (as defined within the GDPR) is held by the company i.e.

- Race
- Religion
- Political Opinion
- Trade Union Membership
- Sexual Orientation
- Biometric Data
- Genetic Data

The only Health information that may be held would be any issues related to inability to carry out certain tasks due to health restrictions as appropriate.

6.2 Data Sources

The data held as defined above, shall be obtained and agreed with the individual only at commencement of employment/engagement during the induction process. The induction shall include a briefing on the requirements of the GDPR and confirmation that the individual accepts and understands the company's policies including this Information Security Policy and that the individual has the right to see the details held at any time on request.

Only data that is required to be held due to legal requirements as defined by the HMRC and/or HSE after the termination of employment /engagement will be retained as per the legislative authority. All other data shall be destroyed as applicable.

It is the individual's responsibility to inform the company of any changes as required. The General Manager will undertake a periodic review of training needs and update the training data as required.

No personal data with be shared with external sources other than the data legally required by the HMRC for tax related issues.

Further Information

Further information and advice on this policy can be obtained from

The Inputgroup General Manager

Telephone 01332 348830 (ext. 24)

Mobile 07801926218

Email k.smith@inputgroup.co.uk

ICO (Information Commissioners Office)

Website – ico.org.uk
helpline on 0303 123 1113.

(*The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals*).

Appendix A

Principles of the General Data Protection Regulations

Principle 1

- Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:
- a) at least one of the conditions in Schedule 2 is met, and
  b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
- Have you identified the purpose of the project?
- How will individuals be told about the use of their personal data?
- Do you need to amend your privacy notices?
- Have you established which conditions for processing apply?
- If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?
- If your organisation is subject to the Human Rights Act, you also need to consider:

Will your actions interfere with the right to privacy under Article 8? Have you identified the social need and aims of the project?
Are your actions a proportionate response to the social need

Principle 2

Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes. Does your project plan cover all of the purposes for processing personal data?

Have potential new purposes been identified as the scope of the project expands?

Principle 3

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

Is the information you are using of good enough quality for the purposes it is used for?

Which personal data could you not use, without compromising the needs of the project?

Principle 4

Personal data shall be accurate and, where necessary, kept up to date.

If you are procuring new software does it allow you to amend data when necessary?

How are you ensuring that personal data obtained from individuals or other organisations is accurate?

Principle 5

Personal data processed for any purpose or purposes shall not be kept for longer than necessary for that purpose or those purposes.

What retention periods are suitable for the personal data you will be processing?

Are you procuring software which will allow you to delete information in line with your retention periods?

Principle 6

Personal data shall be processed in accordance with the rights of data subjects under this Act.

Will the systems you are putting in place allow you to respond to subject access requests more easily?

If the project involves marketing, have you got a procedure for individuals to opt out of their information being used for that purpose?

Principle 7

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Do any new systems provide protection against the security risks you have identified?

What training and instructions are necessary to ensure that staff know how to operate a new system securely?

Principle 8

Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country of territory ensures and adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Will the project require you to transfer data outside of the EEA?

If you will be making transfers, how will you ensure that the data is adequately protected?

Appendix B

A summary of the Data Protection Act 1998

The Data Protection Act sets out eight protection principles which form the legislative framework and with which a data controller must comply.

1. Personal data shall be processed fairly and lawfully.
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 in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose.
6. Personal data shall be processed in accordance with the rights of data subjects under the Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of or damage to personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area.

IMPORTANT - Interpretation of the 7th principle

- The data controller must take reasonable steps to ensure the reliability of any employees who have access to the personal data.
- Where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller must in order to comply with the seventh principle-
  a) Choose a data processor providing sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out, and
  b) Take reasonable steps to ensure compliance with those measures.
- Where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller is not to be regarded as complying with the seventh principle unless-
  a) The processing is carried out under a contract-
  (i) Which is made or evidenced in writing, and
  (ii) Under which the data processor is to act only on instructions from the data controller, and

  b) The contract requires the data processor to comply with obligations equivalent to those imposed on a data controller by the seventh principle.

BREACHES OF THIS ACT MAY RESULT IN CRIMINAL PROCEEDINGS AGAINST THE DATA CONTROLLER AND THE AWARD OF FINANCIAL COMPENSATION TO THE DATA SUBJECT IN RESPECT OF PERSONAL DATA WHICH NOW INCLUDES DATA IN A 'RELEVANT FILING SYSTEM', NOT JUST COMPUTERS.

6. Policy approved by:

Signature  Date 30.04.18

[Adrian Monk, Owner/Director, The Inputgroup.

Client Assurance Policy
(BMS16)

The Input Group is committed to providing clients with sufficient assurance of the company's ability to provide its services of design, construction, refurbishment and maintenance activities for the rail industry and other UK sectors and the design, manufacture and installation of commercial signage. Our core business is to offer a tailored package of services to fulfil specific project requirements.
providing evidence of conformity.

The company are certificated by a UKAS accredited certification body to the following internationally recognised standards i.e. ISO9001 (Quality Management System) : ISO14001 (Environmental Management System) and OHSAS 18001 (H&S Management System) and hold an Integrated Management Systems certificate for all three accreditations.

The company are an Alcumus SAFE contractor (MS3440) and accredited to The Rail Industry Supplier Qualifications Scheme (RISQS) which is subject to an annual audit of the Industry Minimum Requirements (IMR) module. A copy of the RISQS certificate (registration number 2919) can be provided on request.

Documentation

The Input Group will provide the following documentation as a minimum prior to commencement of on-site contract arrangements:

- Copies of our latest Public Liability, Employers Liability and Professional Indemnity insurance certificates.
- A copy of our safety policy and other policies that may be requested.
- The most recent accident & RIDDOR statistics.
- The Input Group provides Risk Assessment Method Statements (RAMS) that are submitted to each client for approval prior to commencement of each project.
- All staff engaged in working on client's premises will be issued with a valid Input Group photographic ID card. All staff will be required to have their ID cards available for examination by the clients at all times. The ID cards issued by The Input Group that will be rescinded on termination of their employment.
- All Input Group staff are briefed on the company's Drugs & Alcohol Policy, which is complient with the rail industry standards, briefed to all staff during company induction. This includes a zero tolerance to being under the influence on site, and being subject to for-cause screening in the event of an accident. The company has a current contract in place for carrying out 'for-cause' screening. Contract can be provided on request.
- All staff provide self certification of medically fittness to carry out their dutues in a live railway environment and are over the age of 18.
- The Input Group can confirm that no-one under the age of 18 will be permitted onto client's sites without prior notification which will includied a submission of a Young Person's Risk Assessment for client approval, as applicable.
- The Input Group can confirm that a robust check on individuals right to work in the UK is carried out in compliance with Immigration, Asylum and Nationality Act and utilises the the Right to Work checklist as issued by the home office.

All the above minimum information will be provided for Input Group staff and subcontractors as applicable. Additional information can be made available on request from each client as applicable.

This Policy Statement is authorised by:

Signed 

Managing Director, Adrian Monk

Date; 21st May 2018

Personal data

The GDPR applies to personal data. This is any information that can directly or indirectly identify a natural person and can be in any format.

The Regulation places much stronger controls on the processing of special categories of personal data. The inclusion of genetic and biometric data is new.

Personal data

Name
Address
Email address
Photo
IP address
Location data
Online behaviour (cookies)

Special categories of personal data

Race
Religion
Political opinions
Trade union membership
Sexual orientation
Health information
Biometric data
Genetic data

Personal data must be processed according to the six data protection principles:

- Processed lawfully, fairly and transparently.
- Collected only for specific legitimate purposes.
- Adequate, relevant and limited to what is necessary.
- Must be accurate and kept up to date.
- Stored only as long as is necessary.
- Ensure appropriate security, integrity and confidentiality.

You must be able to demonstrate compliance with the GDPR:

- The establishment of a governance structure with roles and responsibilities.

- Keeping a detailed record of all data processing operations.
- The documentation of data protection policies and procedures.
- Data protection impact assessments (DPIAs) for high-risk processing operations. Learn more >>
- Implementing appropriate measures to secure personal data.
- Staff training and awareness.
- Where necessary, appoint a data protection officer.

Principle 1

- Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:
- a) at least one of the conditions in Schedule 2 is met, and
- b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
- Have you identified the purpose of the project?
- How will individuals be told about the use of their personal data?
- Do you need to amend your privacy notices?
- Have you established which conditions for processing apply?
- If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?
- If your organisation is subject to the Human Rights Act, you also need to consider:
- Will your actions interfere with the right to privacy under Article 8?
  Have you identified the social need and aims of the project?
  Are your actions a proportionate response to the social need?

Principle 2

Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes. Does your project plan cover all of the purposes for processing personal data?

Have potential new purposes been identified as the scope of the project expands?

Principle 3

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

Is the information you are using of good enough quality for the purposes it is used for?

Which personal data could you not use, without compromising the needs of the project?

Principle 4

Personal data shall be accurate and, where necessary, kept up to date.

If you are procuring new software does it allow you to amend data when necessary?

How are you ensuring that personal data obtained from individuals or other organisations is accurate?

Principle 5

Personal data processed for any purpose or purposes shall not be kept for longer than necessary for that purpose or those purposes.

What retention periods are suitable for the personal data you will be processing?

Are you procuring software which will allow you to delete information in line with your retention periods?

Principle 6

Personal data shall be processed in accordance with the rights of data subjects under this Act.

Will the systems you are putting in place allow you to respond to subject access requests more easily?

If the project involves marketing, have you got a procedure for individuals to opt out of their information being used for that purpose?

Principle 7

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Do any new systems provide protection against the security risks you have identified?

What training and instructions are necessary to ensure that staff know how to operate a new system securely?

Principle 8

Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country of territory ensures and adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Will the project require you to transfer data outside of the EEA?

If you will be making transfers, how will you ensure that the data is adequately protected?

At a glance

- Legitimate interests is the most flexible lawful basis for processing, but you cannot assume it will always be the most appropriate.
- It is likely to be most appropriate where you use people's data in ways they would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing.
- If you choose to rely on legitimate interests, you are taking on extra responsibility for considering and protecting people's rights and interests.
- Public authorities can only rely on legitimate interests if they are processing for a legitimate reason other than performing their tasks as a public authority.
- There are three elements to the legitimate interests basis. It helps to think of this as a three-part test. You need to:
- identify a legitimate interest;
- show that the processing is necessary to achieve it; and
- balance it against the individual's interests, rights and freedoms. The legitimate interests can be your own interests or the interests of third parties. They can include commercial interests, individual interests or broader societal benefits.
- The processing must be necessary. If you can reasonably achieve the same result in another less intrusive way, legitimate interests will not apply.
- You must balance your interests against the individual's. If they would not reasonably expect the processing, or if it would cause unjustified harm, their interests are likely to override your legitimate interests.
- Keep a record of your legitimate interests assessment (LIA) to help you demonstrate compliance if required.
- You must include details of your legitimate interests in your privacy notice.

Checklists

☐ We have checked that legitimate interests is the most appropriate basis.

☐ We understand our responsibility to protect the individual's interests.

☐ We have conducted a legitimate interests assessment (LIA) and kept a record of it, to ensure that we can justify our decision.

☐ We have identified the relevant legitimate interests.

☐ We have checked that the processing is necessary and there is no less intrusive way to achieve the same result.

☐ We have done a balancing test, and are confident that the individual's interests do not override those legitimate interests.

☐ We only use individuals' data in ways they would reasonably expect, unless we have a very good reason.

☐ We are not using people's data in ways they would find intrusive or which could cause them harm, unless we have a very good reason.

☐ If we process children's data, we take extra care to make sure we protect their interests

☐ We have considered safeguards to reduce the impact where possible.

☐ We have considered whether we can offer an opt out.

☐ If our LIA identifies a significant privacy impact, we have considered whether we also need to conduct a DPIA.

☐ We keep our LIA under review and repeat it if circumstances change.

☐ We include information about our legitimate interests in our privacy notice.

How can we apply it in practice?

If you want to rely on legitimate interests, you can use the three-part test to assess whether it applies. We refer to this as a legitimate interests assessment (LIA) and you should do it before you start the processing.

An LIA is a type of light-touch risk assessment based on the specific context and circumstances. It will help you ensure that your processing is lawful. Recording your LIA will also help you demonstrate compliance in line with your accountability obligations under Articles 5(2) and 24. In some cases an LIA will be quite short, but in others there will be more to consider.

First, identify the legitimate interest(s). Consider:

- Why do you want to process the data – what are you trying to achieve?
- Who benefits from the processing? In what way?
- Are there any wider public benefits to the processing?
- How important are those benefits?
- What would the impact be if you couldn't go ahead?
- Would your use of the data be unethical or unlawful in any way?

Second, apply the necessity test. Consider:

- Does this processing actually help to further that interest?
- Is it a reasonable way to go about it?
- Is there another less intrusive way to achieve the same result?

Third, do a balancing test. Consider the impact of your processing and whether this overrides the interest you have identified. You might find it helpful to think about the following:

- What is the nature of your relationship with the individual?
- Is any of the data particularly sensitive or private?
- Would people expect you to use their data in this way?
- Are you happy to explain it to them?
- Are some people likely to object or find it intrusive?
- What is the possible impact on the individual?
- How big an impact might it have on them?
- Are you processing children's data?
- Are any of the individuals vulnerable in any other way?
- Can you adopt any safeguards to minimise the impact?
- Can you offer an opt-out?

You then need to make a decision about whether you still think legitimate interests is an appropriate basis. There's no foolproof formula for the outcome of the balancing test – but you must be confident that your legitimate interests are not overridden by the risks you have identified.

Keep a record of your LIA and the outcome. There is no standard format for this, but it's important to record your thinking to help show you have proper decision-making processes in place and to justify the outcome.

Keep your LIA under review and refresh it if there is a significant change in the purpose, nature or context of the processing.

If you are not sure about the outcome of the balancing test, it may be safer to look for another lawful basis. Legitimate interests will not often be the most appropriate basis for processing which is unexpected or high risk.

If your LIA identifies significant risks, consider whether you need to do a DPIA to assess the risk and potential mitigation in more detail. See our guidance on DPIAs for more on this.

The GDPR provides the following rights for individuals:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

Right to be informed

- he right to be informed encompasses your obligation to provide 'fair processing information', typically through a privacy notice.
- It emphasises the need for transparency over how you use personal data.

What information must be supplied?

The GDPR sets out the information that you should supply and when individuals should be informed.

The information you supply is determined by whether or not you obtained the personal data directly from individuals. See the table below for further information on this.

The information you supply about the processing of personal data must be:

- concise, transparent, intelligible and easily accessible;
- written in clear and plain language, particularly if addressed to a child; and
- free of charge.

The table below summarises the information you should supply to individuals and at what stage.

What information must be supplied?	Data obtained directly from data subject	Data not obtained directly from data subject
Identity and contact details of the controller (and where applicable, the controller's representative) and the data protection officer	✓	✓
Purpose of the processing and the lawful basis for the processing	✓	✓
The legitimate interests of the controller or third party, where applicable	✓	✓
Categories of personal data		✓
Any recipient or categories of recipients of the personal data	✓	✓
Details of transfers to third country and safeguards	✓	✓

Retention period or criteria used to determine the retention period	✓	✓
The existence of each of data subject's rights	✓	✓
The right to withdraw consent at any time, where relevant	✓	✓
The right to lodge a complaint with a supervisory authority	✓	✓
The source the personal data originates from and whether it came from publicly accessible sources		✓
Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data	✓	
The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences	✓	✓

When should information be provided?	At the time the data are obtained.	Within a reasonable period of having obtained the data (within one month)
		If the data are used to communicate with the individual, at the latest, when the first communication takes place; or
		If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.