


<b>Information Classification</b> <b>Document Ref:</b>	 <b>IPL-IS-POL 008</b>	<b>Page:</b> <b>Issue No:</b> <b>Issue Date:</b> <b>Authorised:</b> <b>Title:</b>	1 OF 8 6 15/05/2018 A Burrow Data Protection Policy
---	--	---	---


## Data Protection Policy

### CONTENTS

1.	Contents	1
2.	Version Control	1
3.	Overview	2
4.	Purpose	2
5.	Scope	3
6.	Policy	3

## 2 Version

6	15/05/18	Revised for GDPR	A Burrow	<b>APB</b>
5	11/08/16	Complete rewrite	A Burrow	<b>APB</b>
4	06/05/15	Archiving & storage of data	A Burrow	<b>APB</b>
3	05/09/13	Reviewed	A Burrow	<b>APB</b>
2	07/01/09	Company Name Change	B Gill	<b>BG</b>
1		New Policy Issued	A Burrow	<b>APB</b>
ISS.No.	DATE	REVISION	AUTH.BY	SIG.

<b>Information Classification</b> <b>Document Ref:</b>	 <b>IPL-IS-POL 008</b>	<b>Page:</b> <b>Issue No:</b> <b>Issue Date:</b> <b>Authorised:</b> <b>Title:</b>	2 OF 8 6 15/05/2018 A Burrow Data Protection Policy
---	--	---	---

### 3.0 Overview

Integrity Print has a legal obligation and a reputational interest to appropriately use and safeguard the personal and sensitive data that it has in its possession, and to ensure that it conforms to the requirements of the General Data Protection Regulations (GDPR) and all other applicable data protection laws.

A range of products and services that Integrity Print provides to its customers are orientated around data processing and data management, so it is imperative that all employees and, where applicable, contractors and other third parties are aware of the data protection requirements associated with each contract, and that these are fulfilled in compliance with the regulations.

This policy should be read in conjunction with the Data Exchange Policy and with the Integrity Print Terms and Conditions of Sale and Terms and Conditions of Purchase. These documents may be accessed via the Integrity Print website ([www.integrity-print.com](http://www.integrity-print.com))

### 4.0 Purpose

The purpose of this policy is to explain the principles of data protection and outline the good practices and procedures that employees and contractors should follow when working with personal and sensitive data.

The key concerns relating to personal and sensitive data are guarding against inappropriate use and data loss / leakage; incidents may be caused by poor process controls, by negligence or by malicious actions.

Data protection issues have a very high profile in the public consciousness, in the media, and amongst commercial and legislative bodies. Therefore, the implications of a data protection incident for Integrity Print are extremely serious.

Depending on the nature of an incident, Integrity Print could be subject to a punitive fine that, in the most serious circumstances, could threaten the viability of the business.


In addition to any financial penalty, our reputation with our customers would be seriously damaged, making it difficult to retain repeat work and win new orders.

It is in every employee's best interests to ensure that this policy is adhered to.

Integrity Print considers this policy to be extremely important. If you are found to be in breach of the policy, then you are liable to be disciplined in accordance with the disciplinary procedure. In certain circumstances, breach of this policy may be considered gross misconduct resulting in the immediate termination of your employment.

If there is anything in this policy that you do not understand, you should notify your manager immediately and seek clarification.

Employees will be informed when this policy is amended, but it is the responsibility of each individual employee to ensure that they have read and understood the latest version of this document, and to ensure that its rules are applied.

	<b>Page:</b> 3 OF 8 <b>Issue No:</b> 6 <b>Issue Date:</b> 15/05/2018 <b>Authorised:</b> A Burrow <b>Title:</b> Data Protection Policy
<b>Information Classification</b> <b>Document Ref:</b> IPL-IS-POL 008	

## 5.0 Scope

Data protection legislation is designed to protect the privacy and integrity of data held on individuals by businesses and other organisations.

In the context of the data held by integrity Print this includes:

- Data that relates to employees
- Data that relates to the individuals who work for our customers and suppliers
- Data relating to the recipients of the transactional communications that we process on behalf of our customers

In the terminology of the legislation, Integrity Print is a *Data Controller* for the first two categories; that is, Integrity Print collects the data for its own defined business purposes (ie: for the first, HR and payroll, and for the second, support for sales and purchasing).

In respect of the third category, Integrity Print is a *Data Processor*; in that we process data on behalf of our customers, having no part in designing or ensuring the legitimacy of the business purpose.

In any given situation, irrespective of whether we are acting as a Data Controller or a Data Processor, Integrity Print is responsible for protecting all of the personal and sensitive data within its possession. Some definitions:

<i>Data</i>	Information processed by computer or recorded as part of a manual filing system. The manual files need to be structured, ie. so that specific information about a particular individual can be found easily.
<i>Personal Data</i>	Data which relates to a living individual who can be identified from the data (even where that information is only held on that person in their capacity as the representative of a customer or supplier).
<i>Privacy Notice</i>	The details of the personal information that Integrity Print holds in its role as a data controller can be determined by viewing the relevant privacy policy.

## 6.0 Policy

6.1 Integrity Print will comply with the requirements of GDPR, as summarised below:

6.1.1 Under GDPR there are six principles that are set out as the main responsibilities for organisations. These are:

- 1<sup>st</sup> Personal data must be processed lawfully, fairly and in a transparent manner in relation to individuals;
- 2<sup>nd</sup> Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- 3<sup>rd</sup> Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;

**2****Information Classification****Document Ref:****IPL-IS-POL 008****Page:** 4 OF 8  
**Issue No:** 6  
**Issue Date:** 15/05/2018  
**Authorised:** A Burrow  
**Title:** Data Protection Policy

4<sup>th</sup> Personal data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay;

5<sup>th</sup> Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;

6<sup>th</sup> Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.”

6.1.2 GDPR places accountability upon the organisations controlling and processing the personal data; an approach must be taken whereby data protection is provided ‘by default and design’. Accountability obligations are ongoing, organisations must review and where necessary update the measures in place.

6.1.3 GDPR introduces additional responsibilities and legal controls in relation to the processing of Special Category Data (where this includes such information as race; ethnic origin; politics; trade union membership; generics; biometrics; health; sex life or sexual orientation).

6.1.4 GDPR introduces additional controls in relation to the processing of Criminal Offence Data.

6.1.5 GDPR introduces specific rights for individuals whose data may be processed, this includes:

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

6.1.6 GDPR stipulates that personal data may only be transferred outside of the UK and European Union if the Commission has decided that area ensures and adequate level of data protection.

6.1.7 GDPR introduces a duty on all organisations to have robust procedures to detect, investigate and record of all personal data breaches; and a requirement to report certain types of personal data breaches to the relevant supervisory authority

**2****Information Classification****Document Ref:****IPL-IS-POL 008**

<b>Page:</b>	5 OF 8
<b>Issue No:</b>	6
<b>Issue Date:</b>	15/05/2018
<b>Authorised:</b>	A Burrow
<b>Title:</b>	Data Protection Policy

## 6.2 Data held on employees

- 6.2.1 Employees should be aware that personal data relating to them will be collected and used by Integrity Print to administer their employment contract and remuneration; and to ensure that issues including, but not restricted to, health and safety, skills and training, time and attendance, disciplinary matters etc are effectively managed.
- 6.2.2 By signing their employment contract, the employee acknowledges that their personal information may be held by Integrity Print, insofar as it complies with the principles described in 6.1.
- 6.2.3 If the employee's personal situation changes, they should contact the HR Manager to ensure that their records are updated to maintain accuracy.
- 6.2.4 Employees have the right, on written request to the Company Data Protection Officer to be supplied with a copy of any personal data held about them, to be advised of to whom the data has been disclosed, and where appropriate to have that data corrected or erased.

## 6.3 Data held on customers and suppliers

- 6.3.1 Integrity Print will maintain the contact details of the individuals associated with its customers and suppliers for the purpose of customer and supplier relationship management in the pursuance of its existing trading contracts and agreements.
- 6.3.2 It should be noted that the 4<sup>th</sup> principle of the legislation requires that such information is accurate and kept up to date.

## 6.4 Data held for marketing purposes

- 6.4.1 Integrity Print will maintain marketing databases which will contain the contact details of individuals who are associated with prospective business-to-business customers. Such records as are collected and maintained will be appropriately targeted as likely users of Integrity Print's products and services.
- 6.4.2 Access to employee, customer, supplier and marketing databases will be restricted and only made available to those employees whose role within the business requires it.

## 6.5 Data Controller

- 6.5.1 In our capacity as a Data Controller, Integrity Print will follow the guidelines as set out in clause 6.1 of this document and will ensure that any contracted sub processors will: -
- 6.5.2 Ensure any third-party process will provide guarantees that the data supplied will be protected.
- 6.5.3 Personal data will be protected by implementing technical or organizational measure in accordance to EU GDPR.

<b>Information Classification</b>	<b>2</b>	<b>Page:</b>	6 OF 8
<b>Document Ref:</b>	<b>IPL-IS-POL 008</b>	<b>Issue No:</b>	6
		<b>Issue Date:</b>	15/05/2018
		<b>Authorised:</b>	A Burrow
		<b>Title:</b>	Data Protection Policy

6.5.4 A Data Processing Impact Analysis (DPIA) has been carried out to ensure affective control of data.

6.5.5 All personnel data will be kept accurate and, kept up to date

6.5.6 To return or destroy any data received on request.

## 6.6 Data Processing on behalf of customers

6.6.1 The product, output and any related services that Integrity Print has been engaged to provide by agreement with our customer should be documented in each case. The documentation should make it clear that Integrity Print is acting in the capacity of a Data Processor, not as the Data Controller.

6.6.2 It is likely that we will be under obligations to our customer in relation to the management of data under the terms of our contract with them. Commonly a contract may include obligations such as those below. All such specific instructions should be documented, disseminated and complied with by all involved in fulfilment.

- to hold the data separately.
- not to transfer or disclose the data to any third party without authority
- to provide the data with adequate security against loss, damage or destruction
- to return or destroy any data received on request.
- to destroy the data after a defined period of time.
- to allow the data controller to audit our data protection procedures

## 6.7 Sub-contracting

In certain instances, Integrity Print may outsource the responsibility for the data processing. In such cases the supplier acts as our data processor and may only act on our express instructions in relation to the data we supply to them and should not use the data for any other purpose or disclose it to anyone else.

Under the Act, these restrictions should be set out in a written data processor contract.

When allowing others access to the customer data and to process data on our behalf we should ensure that the third-party data processor provides sufficient guarantees in respect of the security measures they are required to take.

## 6.8 Storage and handling of personal and sensitive data

6.8.1 Where personal and sensitive data is held in manual filing systems, the relevant department manager will be responsible for ensuring that their staff are aware of the associated data protection issues, and that the records are adequately protected and comply with current data protection requirements.

<b>2</b>	<b>Page:</b> 7 OF 8 <b>Issue No:</b> 6 <b>Issue Date:</b> 15/05/2018 <b>Authorised:</b> A Burrow <b>Title:</b> Data Protection Policy
<b>Information Classification</b>  <b>Document Ref:</b> IPL-IS-POL 008	

- 6.8.2 As described in the Data Exchange Policy, data received from customers for processing on their behalf will be stored entirely within the bounds of the local area network at the Integrity Print site.
- The storage of sensitive information is restricted to Integrity Print's servers, where access to the relevant folders is limited to those staff who require it for their specific job roles and who have been authorised to have access by the appropriate Information Security Owner.
  - Data will be stored on servers in an unencrypted state to ensure compatibility with Integrity Print's production software, equipment and processes.
  - The security of the network and server environment is the responsibility of the IT Manager, who will ensure that access control is maintained and that appropriate measures are taken to reduce the risk of data leakage.
  - The security of data during the manufacturing stages of data preparation, data processing and fulfilment will be the responsibility of the Directors responsible for sales and production, the Transactional IT department, and the Security & Transactional Print Manager.
  - Unless otherwise specified by the customer, data will be stored for period of 90 days after the completion of production for quality, audit and regulatory purposes. It will then be deleted by an automated script.
- 6.8.3 Integrity Print employees are not permitted to store personal or sensitive information on the hard drives of desktop PCs, laptops or other mobile devices and must not make or transfer copies of files to removable media (CDs, memory sticks etc).
- 6.8.4 Data protection requirements must be taken into consideration before any decision is made to store personal or sensitive data on a third party hosted system or maintain or access such data via an online application.
- See policy IPL-IS-POL 016 Use of Online Applications and Internet Services
  - Where a customer instructs us to send the output from the processing that we carry out on their behalf to a third party hosted system, this should be documented to make it clear that the responsibility for the data protection issues associated with the hosted site lays with the customer.

## 6.9 Data subject access policy

The *Data Subject* is the individual who Integrity Print is holding personal or sensitive information about. In our capacity as a Data Controller, the data subject will be an employee, a customer or a supplier, whilst as a Data Processor the data subject will be a person included in the data that we will process on behalf of one of our customers.

The rights of the Data Subject are outlined in clause 6.1.5

All data subject access requests received by Integrity Print must be advised to the Company Data Protection Officer (email to: [dpo@integrity-print.com](mailto:dpo@integrity-print.com)).

<b>Information Classification</b>	<b>2</b>	<b>Page:</b>	8 OF 8
<b>Document Ref:</b>	<b>IPL-IS-POL 008</b>	<b>Issue No:</b>	6
		<b>Issue Date:</b>	15/05/2018
		<b>Authorised:</b>	A Burrow
		<b>Title:</b>	Data Protection Policy

## 6.10 Integrity Print websites - cookie statement

Where cookies are used on a website, there is a requirement to present a 'cookie statement' on the first occasion that a person accesses the site. Cookies are small programs that are placed on a visitor's device to collect information about their device and their use of the site. The statement must advise the nature and purpose of the cookie so that the visitor can make an informed decision on whether to proceed.

Employees who are involved in the design and implementation of Integrity Print websites must ensure that this requirement is satisfied.

## 6.11 Integrity Print data protection registration

Integrity Print is registered with the Information Commissioner's Office  
The company registration number is: Z1440935

## 6.12 Liability

In its role as a Data Processor for its customers, or where as a Data Controller Integrity Print has contracted with a third party to provide sub-processing services in relation to personal data, Integrity Print will not be liable for any loss, unauthorised disclosure or other data breach if an external party acts in a manner that fails to comply with this policy.

Further details are available in the Integrity Print documents:

- Terms and Conditions of Sale
- Terms and Conditions of Purchase