GDPR POLICY AND PROCEDURES MANUAL

Index

Section 1 SCOPE, OBJECTIVES AND RESPONSIBILITY

1.1 SCOPE

This policy manual defines the GDPR policies adopted by all companies within the Family of Businesses (the few exceptions are detailed within the respective policy narratives).

1.2 OBJECTIVES

The objectives of these policies are to:-

1. Ensure that a uniformity of approach is achieved throughout the Family of Businesses and the avoidance of inconsistencies.
2. To provide concise guidelines to managers.
3. To ensure that the company complies with best commercial practice and in accordance with current legislation.
4. To provide the policy statements against which the Internal Audit functions measure the controls of the respective Group companies.

1.3 RESPONSIBILITIES

The respective Group Boards are responsible for maintaining, reviewing and approving these policies. Any amendments must be approved by all Boards prior to implementation.

Section 2 GDPR POLICIES AND PROCEDURES

2.1 Subject Access Request Procedure

Under the GDPR existing staff, ex-employees, previous job applicants and customers may request access to information held about them free of charge (SAR).

This may include information held both electronically and manually and will therefore include personal information recorded within electronic systems, personnel files, personnel database, spreadsheets, e-mails (in line with our e-mail retrieval policy), accident books, private health files, databases or word documents and may also be in the form of photographs and CCTV images etc.

The request must be made in writing and must be responded to without delay and at the latest within one month of receipt of the request. This time can be extended by a further 2 months where requests are complex or numerous. However if this is the case you must inform the individual within one month of the receipt of the request and explain why the extension is necessary.

An individual is entitled to be told whether any personal data is being processed; given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people; given a copy of the personal data; and given details of the source of the data (where this is available).

All HR-related SAR requests received must be forwarded to the relevant HR department without delay in order for it to be processed within the legal timescale.

Where information in respect of other individuals is contained within the information requested it should not be disclosed without the consent of that individual.

Routine on-going business additions and amendments may be made to the personal information after a request is received. However the information must not be altered as a result of receiving the request, even if the record contains inaccurate or embarrassing information, as this would be an offence under the Data Protection Act 1998.

A copy of the information should be supplied to the applicant electronically.

2.2 Data Erasure Request Procedure

The GDPR introduces a right for individuals to have personal data erased. This right to erasure is also known as 'the right to be forgotten'. Individuals, whether employees, ex-employees, previous job applicants or customers can make a request for erasure verbally or in writing and the Company will respond to their request within 1 month. This right is not absolute and only applies in certain circumstances.

The Company will not erase data which it feels necessary to hold to carry out legal obligations or for the establishment, exercise or defence of legal claims.

Where the Company does agree to erasure, the following data will be erased:

- Relevant documents/information from the personnel file
- Relevant documents/information held by the line manager.
- A copy of relevant information held electronically in relevant database programs (e.g. SDM, Querypad etc.)
- Relevant emails resulting from an email system search in line with our email retrieval policy (see 2.4)

Where the Company has disclosed this information to others, the Company will contact those organisations and request that they also erase relevant data.

2.3 Data Loss/Breaches Procedure

The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority within 72 hours of becoming aware of the breach, where feasible.

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, the Company will also inform those individuals without undue delay.

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

All suspected breaches of personal data must be reported to the company's GDPR officer, GDPR Steering Committee member or Main Board Director. Each breach will be assessed on its merits to ascertain whether or not it contains personal data and whether or not it requires reporting to the Information Commissioner's Office (ICO).

When a personal data breach has occurred, the Company will establish the likelihood and severity of the resulting risk to a data subject's rights and freedoms. Higher level severity includes personal data relating to medical conditions, date of birth, disciplinary issues and remuneration, whereas lower level severity includes home address and telephone number. If it's likely that there will be a risk then the Company will notify the ICO. If it's unlikely then it will not be reported. However, where a decision is made not to report the breach, the justification for this should be documented.

All breaches of personal data will be added to the relevant company's data breach record log.

When reporting a breach to the ICO, the Company will provide:

A description of the nature of the personal data breach including, where possible:

- The categories and approximate number of individuals concerned
- The categories and approximate number of personal data records concerned
- The name and contact details of the GDPR Officer or other contact point where more information can be obtained
- A description of the likely consequences of the personal data breach
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

For further guidance on what level of reporting is required for a data breach, please see **Appendix 1 Reporting a Data Breach – Process Flow.**

2.4 Email Retrieval/Access Policy

Users' mailboxes are not private as IT systems logging and monitoring will take place where appropriate, access may be given to a manager/other user if that individual is on holiday or ill and IT may also be asked to run searches through the email archive to bring back emails from current or ex-employees. All data that is created and stored on Company systems is the property of the Company and there is no official provision for individual data privacy.

For further information, please see the IT User Policy in section 12.2.of the Employee Handbook.

Any breach of personal information must be reported to the Information Commissioner's Office (ICO) in the usual way, as per the details contained in the Data Loss/Breaches procedure.

2.5 Employee Communication

With effect from 25th May 2018, all employees will have a clause relating to GDPR included in their Terms and Conditions of Employment, referring to the Privacy Notice contained within the Employee Handbook (section 12.1) and will also receive GDPR training appropriate to their position, .ie staff who process significant amounts of personal data as part of their job duties will be required to undertake an on-line training course, other staff with limited access to personal data will sign an internal training document. Production staff will, in general, not be required to undertake GDPR training.

2.6 Recruitment Privacy Policy

Personal data collected during the recruitment process will be used for recruitment purposes only and is therefore for a legitimate business interest.

Data is collected via on-line searches, application forms, CVs and covering letters/e-mails, sent either direct or from recruitment agencies, and received either speculatively or in response to a job advert.

The Company uses the data to screen candidates and to judge their suitability to progress to interview. Data may be stored in spreadsheets, on an Applicant Tracking System or in e-mail folders, or where in paper form, in locked cabinets within the HR department and these may be shared with the relevant hiring team.

The data of unsuccessful candidates will be stored for a maximum of 12 months, after which it will be deleted as far as is practically possible. The Company will not store data for longer than this period without contacting the candidate to ask for permission first.

Where candidates are sourced on-line, the Company will only retain this information where it intends to contact those candidates. We will not retain a candidate's details for longer than a month without contacting them. If the Company changes its mind and decides not to contact the individual it will delete the data immediately.

Candidates have the right to be kept informed about the processing of their data, the right to be forgotten, to rectify or access their data, to restrict processing or to withdraw their consent. Please contact the HR department to make such requests. Any requests to delete, access, rectify or stop processing data will be carried out within one month of the request.

2.7 Privacy Notice for Employees – see Employee Handbook section 12.1

2.8 CCTV Policy – see Employee Handbook section 14.5

2.9 Information Storage Policy

Routine archiving should and must continue throughout the year. Where this is not carried out, at the end of each financial year, a schedule of documents to be archived (as required in Document Type Retention Requirements page) and timetable for archiving is agreed to complete within 28 days of financial year end.

All Department Directors/'Directors of' must undertake continuous monitoring of relevant legislation, and are responsible for advising the Board of Directors of impending changes. Thereafter this Policy document must be reviewed, updated as necessary and submitted for approval by the relevant Director/'Director of'.

Archive Data
Archive data is either placed in Central Archive or retained in a dedicated Archive Folder within the Business/Department/Team Areas listed below in 'Master Lists'

See 'Document Type Retention Requirements' page for list of documents to archive and storage periods.
Archive Data Retention Maintenance and Responsibility

The Director/'Director of'/Manager responsible for a Team Area/Business Area listed in Master Lists below is responsible for ensuring appropriate documentation is archived in the first place and continued readability of Archive Data thereafter. See Archive Data Continued Readability Guidelines.

The 'Director of IT' is responsible for ensuring retention of stored archive data, and that it is secure, backed up and accessible.

Archive Data Continued Readability Guidelines
To ensure continued access to historical data and without excessive labour, it is suggested only the following formats are used (other formats are used only with written approval from a Board Director).
PDF - Because this format is a 'picture' of whatever is scanned or saved, it is likely to have longer term uninterrupted accessibility and would be simpler to create readers if required, therefore updating of data is likely to be less frequent. Estimated 10 to 15-year upgrade cycle.
J-PEG - This is a picture format and above notes on pdf are applicable.
Excel - it may be necessary to retain archive information in a format that has formula, hidden data etc and therefore a 'picture' saved on pdf or J-PEG would not be suitable. As excel is the Group preferred spreadsheet software, this or any other similar Team Area Director/Director of/Manager approved software can be used in 'Archive', but is likely to need more regular conversion of Excel archived data to latest version of software. Estimated 5 to 10-year upgrade cycle.
Microfiche - This is old technology and requires more detailed filing to avoid lengthy searches to find what is required. However, at over 100 years (if stored appropriately to avoid degradation) makes easier archiving. Although there is an additional up front cost, there are savings by not requiring periodic (10 – 15 years) upgrade of data to latest software versions.
Bespoke In-House and 'Bought in' Programs (new and existing) - User Beware, (Team Area/ Business Area Director/Director of/Manager). If data generated from these programs are destined for Indefinite Archive, assurances must be sought to ensure data can be accessed after cessation of use or following significant upgrades. The 'Director of IT' will advise of any currently used software programs that are subject to a significant upgrade that may necessitate a conversion of Archive Data to the new software upgrade.

Master Lists
Family of Businesses
Group Archive Employers Liability History 1961 Onwards.

Group Archive security safe list.
Group Archive Hammond Suddards
Group Archive Register of Deeds

Documents accessed through Policy Manual/Policy Manual Support Data/05.04 Management Policies Archive Lists (Password protected, for access contact a Director or Group HR/Payroll Administrator).

Willan Investments and Willan Group:

Willan Investments and Willan Group Retained Documents Master List is accessed via the Subsidiary Data Link on the Intranet, Leading to WI/WG 'Archive Plan'.

Password Protection to apply with authority from WGL directors.

Should any specific means of archiving speciality documents such as Deeds and large plans prove practicable and improve the company's position, this will not be precluded and will be at the discretion of relevant director.

Closomat Group.

COM Group Retained Documents are found on the Group Intranet, Closomat Quality Section, Shared Folder, 'Office' Folder. Or copy this URL into the Intranet Browser:-

\\192.168.1.249\Management\BPD\BPD Quality /Closomat\Quality

Building Product Design Ltd

Health & Safety, Environmental and related Master List is accessed via Intranet Browser:-
\\192.168.1.249\Management\Willan Group\Willan Group H&S Manual\HS&E Information Storage\

Quality Management Procedures and related Archive Lists via Intranet Browser :-
\\192.168.1.249\Management\BPD\BPD Quality

Accounts archive data is accessed via Department request.

Marketing archive data is accessed via Team Area on the BPD Network

Sales Administration archive data is accessed via Team Area on the BPD Network

Operations archive data is accessed via Team Area on the BPD Network

HR archive data is accessed via Team Area on the BPD Network

All above Team Area's are accessed using the following IP address ' \\192.168.1.216\ '

Pinxton (non H&S/Environmental) archive data is accessed via 'GV2 - 192.168.0.5'

Note: Some bulky historical documents may be retained on pallets or/and in storerooms as part of indefinite retention or/and digitised. Documents containing personal information must be kept in locked storerooms with restricted access. This will be documented and safe storage continued. The Production Director is responsible for this activity.

Secure Storage Responsibility

It is the responsibility of the 'Director of IT' to ensure the stored data and archive data is secure, backed up and retrievable, and manages without loss conversion to any future replacement technologies.

DOCUMENT TYPE RETENTION REQUIREMENTS

DOCUMENT TYPE	OPERATIONAL RETENTION REQ	ARCHIVE REQUIREMENTS
INCOME TAX/ PAYE	Retain for 7 years	
	Retain as original documents or copied as Readability Guidelines	
VAT RECORDS	Retain for 7 years	
	Retain as original documents or copied as Readability Guidelines, but note that Customs and Excise have right of refusal for non-original documents.	
INVOICES	Retain for 7 years	
	Retain as original documents or copied as Readability Guidelines	
CORRESPONDENCE/and ADMIN CORRESPONDENCE, WRITTEN and EMAIL, and ORDER PROCESSING RECORDS	Retain for 7 years	Correspondence, written or email that are contractual or concerning a contract are treated as All Contract Documents.
	Retain as original documents or copied as Readability Guidelines after 12 months.	
ALL MARKETING CORRESPONDENCE, WRITTEN and EMAIL, DOCUMENTS, PHOTOGRAPHS, LITERATURE and PRODUCTION DOCUMENTS and UPDATES	Retain as a minimum as original during period of Compilation / Works. Then as maximum as original up to 7 Years.	100 years
		Once Compiled / Works complete, retain originals in secure storage where required, and copies/digital data as Readability Guidelines.
ALL CONTRACT	During period of Compilation / Works	100 years

DOCUMENTS/ FOLDERS INCLUDING ELECTRONIC COMMUNICATIONS (email etc) and all DOCUMENTS UNDER SEAL,		Once Compiled / Works complete, retain originals in secure storage, and copies in electronic/digital software and as Readability Guidelines. For BPD Contract/Quasi Contract data see appendix 3. Retain in Secure Storage/Safe – Pinxton prior to merge of Glidevale and Willan Building Services, and Sale for all other. COM Group retained at Building 1 Brooklands Place, see COM Group Master List link below.
HEALTH & SAFETY and ENVIRONMENTAL (General documentation)	During period of Compilation / Works and Maximum of 3 Years for Electronic/Non Digital documents	100 years Preferred storage is on non re-writeable electronic/digital software and as Readability Guidelines, paper documents not scanned at time of operation to be archived on non rewriteable electronic/digital media as Readability Guidelines within 3 years.
HEALTH & SAFETY and ENVIRONMENTAL (Original incident / accident report files)	During period of Compilation / Works and Maximum of 3 Years for Electronic/Non Digital documents	100 years Preferred storage is on non re-writeable electronic/digital software and as Readability Guidelines, paper documents not scanned at time of operation to be archived on non rewriteable electronic/digital media as Readability Guidelines within 3 years.
HEALTH INSURANCE FILES	Up to 3 years	Destruction or archiving as Readability Guidelines subject to written Board Director approval.
PERSONNEL RECORDS	Period of employment plus five years.	100 years Following operational period, scan to non rewriteable electronic/digital software and retain 100 years, as Readability Guidelines. See appendix 1, Document Retention Storage in Detail by Type, for Personnel documents to be scanned.
EMPLOYERS and PUBLIC LIABILITY	Indefinitely	100 years Retain originals in secure storage and copy to electronic/digital software as Readability Guidelines.
QUALITY RECORDS See Appendix 2 for Guide Definition of a Quality Record.	Retain for 7 years Retain as original documents or copied as Readability Guidelines	
MACHINE MAINTENANCE (including LIFTS) Including lease or hire equipment including Fork Trucks and Access Equipment	During period of Compilation / Works	100 years Following operational period, retain as original documents and on electronic/digital software as Readability Guidelines.
PRODUCT SAMPLES and ASSOCIATED RECORDS	During period of Compilation / Works	100 years Following operational period, retain as original documents and on electronic/digital software as Readability Guidelines.
SURFACE COATING RECORDS All	During period of Compilation / Works	100 years Following operational period, scan/save to electronic/digital software as Readability Guidelines.
PRODUCT SPECIFICATIONS	During period of Compilation / Works	100 years Following operational period, scan/save to electronic/digital software as Readability Guidelines.
GENERAL RECORDS	Determine if required to save for 100 years	100 years

Records not included in all other areas.	from Senior Manger	Following operational period, scan/save to electronic/digital software as Readability Guidelines.

Further Guidance
Appendix 1
Document Retention Storage in Detail by Type
HR Records

'HR records data to be archived'

- Starter Form
- Leaver Form
- Relevant pension correspondence
- Private medical insurance application forms/claim notifications
- SSP, self-certificates, medical certificates, OH reports
- Punctuality / attendance records
- Relevant disciplinary/grievance information
- Relevant redundancy information
- Application forms/CVs
- Equal opportunities forms
- Disability confirmation forms
- Accident at work documents
- Contract of Employment/Change of terms
- Training records

Appendix 2
Guide Definition of a Quality Record
Quality Records (examples)

Records such as

- QMS audit reports
- Calibration of test and measuring equipment
- Inspections
- Tests
- Approvals
- Concessions etc ensure that a company is capable of proving the effectiveness of its QMS
- Records provide objective evidence of activities performed or results achieved

Appendix 3
BPD Quotation and Contractual Documentation Storage
BPD Team project/quotation/quasi contract data is saved on the Network (enabling back up and long-term data storage management by IT). Access to data is via a 'Look Up' program(s) and alternately via Sales Data Management (SDM) programme which has a link to all data relevant to the project.

Appendix 1 Reporting a Data Breach – Process Flow