

Data Protection Policy





Contents

Revision History	3
Approval.....	3
1. Introduction.....	4
2. Personal Data Definition.....	4
3. Why this Policy Exists.....	4
4. Purpose of this Policy	4
5. Responsibility for Compliance with the GDPR.....	5
6. Right to be Informed	6
7. Subject Access Requests.....	6
8. Rectification and erasure	6
9. Disclosure and Sharing of Personal Information	7
10. Training	7
11. Data Storage	7
12. How to Complain	7

Document	Authorised by	Issue/ Rev	Date	Page
EWG-Q-P-04 – Data Protection Policy	EDB	1b	Sept 2019	2 of 7

Data Protection Policy



Revision History

Version	Date	Revision Author	Summary of Changes
1a	16 Jul 18	S. Rowe	1 st issue

Approval

Jeremy Hartley Managing Director Eric Wright Group	Signed  Date: 16 July 2018	 ERIC WRIGHT GROUP
John Wilson Managing Director Eric Wright Construction	Signed  Date: 16 July 2018	 ERIC WRIGHT CONSTRUCTION <small>PART OF THE ERIC WRIGHT GROUP</small>
Diane Bourne Managing Director Eric Wright Civil Engineering	Signed  Date: 16 July 2018	 ERIC WRIGHT CIVIL ENGINEERING <small>PART OF THE ERIC WRIGHT GROUP</small>
Neal Whittle Managing Director Eric Wright Water	Signed  Date: 16 July 2018	 ERIC WRIGHT WATER <small>PART OF THE ERIC WRIGHT GROUP</small>
George Lilley Eric Wright Facilities Management	Signed  Date: 2 nd September 2019	 ERIC WRIGHT FACILITIES MANAGEMENT <small>PART OF THE ERIC WRIGHT GROUP</small>
Karen Hirst Managing Director Maple Grove Developments	Signed  Date: 16 July 2018	 MAPLE GROVE DEVELOPMENTS <small>PART OF THE ERIC WRIGHT GROUP</small>
Christine Winstanley Managing Director Eric Wright Health and Care	Signed  Date: 16 July 2018	 ERIC WRIGHT HEALTH AND CARE
Colin Hetherington Managing Director Applethwaite	Signed  Date: 16 July 2018	 applethwaite

Document	Authorised by	Issue/ Rev	Date	Page
EWG-Q-P-04 – Data Protection Policy	EDB	1b	Sept 2019	3 of 7

Document un-controlled once printed. Please refer to the management system for the latest version.



1. Introduction

The General Data Protection Regulation (GDPR) in force from 25 May 2018 regulates the way that personal data relating to individuals is held and processed. The Data Protection Act 2018 (DPA 2018) incorporates the requirements of GDPR.

In order to operate efficiently Eric Wright Group and its subsidiary companies (the Group) need to collect and use information about people with whom we work whether they be our employees, our advisors, our suppliers, or subcontractors or our customers.

2. Personal Data

Personal Data is information about an individual which enables any person with access to that information to identify the individual concerned such as names, postal addresses, email addresses and telephone numbers together with other information regarding their health, relation, political opinions, criminal records, sexual orientation, racial or ethnic origins, employment history and other such similar details, including opinions about the individual.

3. Why this Policy Exists

The Group takes its responsibilities in processing such information very seriously with a view to protecting the rights of the individuals and maintaining the confidence of our employees and the people with whom we work. We fully endorse and adhere to the principles of the DPA 2018, which are that personal information must:

1. be processed fairly, lawfully and in a transparent manner
2. be collected only for specified explicit and legitimate purposes and not be used for a purpose for which it was not collected
3. be adequate, relevant and limited to what is necessary in relation to the purposes for which it was collected and is processed
4. be accurate and kept up-to-date
5. not be kept for longer than is necessary for the purposes for which it was collected
6. be kept secure using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss destruction or damage
7. not be transferred to another country without appropriate safeguards being in place to protect the information
8. be made available to the persons to whom it relates in accordance with the requirements of the DPA 2018

4. Purpose of this Policy

The purpose of this policy is to ensure that all those people who handle personal information within the Group are fully aware of the requirements of the Act and that

Document	Authorised by	Issue/ Rev	Date	Page
EWG-Q-P-04 – Data Protection Policy	EDB	1b	Sept 2019	4 of 7



they comply with data protection procedures but also that individuals whose data is processed are aware of their rights under the DPA 2018.

5. Responsibility for Compliance with the GDPR

The Group Managing Director and the Board of Directors of the Group have overall responsibility for compliance with the DPA2018 but individual members of staff are responsible for the proper processing of the data which the Group holds.

To this end all these parties will:

- value the personal information entrusted to the Group and make sure they respect that trust;
- go further than just the letter of the law when it comes to handling personal information, and adopt good practice standards;
- consider and address the privacy risks first when they are planning to use or hold personal information in new ways, such as when introducing new systems;
- be open with individuals about how we use their information and who it is given to;
- make it easy for individuals to access and correct their personal information;
- keep personal information to the minimum necessary and delete it when it is no longer needed;
- have effective safeguards in place to make sure personal information is kept securely and does not fall into the wrong hands;
- provide training to staff who handle personal information and treat it as a disciplinary matter if they misuse or do not look after personal information properly;
- put appropriate financial and human resources into looking after personal information to make sure the Group can live up to its promises; and
- regularly check that they are living up to these promises.

The Data Protection Co-ordinator is Phillip Richardson who has the responsibility for:

- carrying out data protection risk assessments and compliance audits
- formulating a privacy risk register
- reviewing data protection procedures and policies
- handling data protection questions from those responsible for adherence to this policy
- keeping the Board informed about data protection responsibilities, risk and issues

The IT Manager Steven Lee who is responsible for:

- ensuring all IT systems, services and equipment used for storing and transferring data meet acceptable security standards
- performing regular checks and scans to ensure security hardware and software is functioning properly
- evaluating any third party services the Group is considering using to store or process data such as cloud computing services

The Human Resources Manager is Sandra Cadman who is responsible for:

- arranging training for staff who process personal data
- managing the processing of personal data relating to employees of the Group

Document	Authorised by	Issue/ Rev	Date	Page
EWG-Q-P-04 – Data Protection Policy	EDB	1b	Sept 2019	5 of 7



The Group Financial Director is Gill Chadwick who is responsible for

- managing the processing of financial transactions to employees of the Group
- managing the processing of financial transactions for clients of Sceptre Nursery
- managing the processing of financial transactions for clients of Water Park

6. Right to be Informed

Individuals have the right to be informed about the collection and use of their personal data and we will provide privacy information in clear and plain language to individuals at the time when we collect their personal information from them or as soon as possible after receiving it from other sources.

7. Subject Access Requests

All individuals whose personal data is processed by the Group are entitled to

- ask what information the Group holds about them and why
- ask how to gain access to it
- be informed how to keep it up to date
- be informed how the Group is meeting its data protection obligations

Such applications are called subject access requests. The subject access request procedure is set out in document EWG-Q-MP-042 - Subject Access Request.

Subject access requests should be made to the Data Protection Co-ordinator by post to Sceptre House, Sceptre Way, Bamber Bridge, Preston PR5 6AW or by email to dataprotection@ericwright.co.uk

There is no fee payable for a subject access request unless the request is manifestly unfounded or excessive in which case a reasonable fee may be charged.

The information will be provided without delay and at the latest within one month of receipt of the request.

The Group will always use reasonable means to verify the identity of anyone making a subject access request before handing over any information.

If the request is made electronically we will provide the information in a similar format.

The person responsible for policies and procedures to deal with requests from individuals to see data obtained by or from CCTV systems operating in premises managed by companies within the Group is the Data Protection Co-ordinator.

8. Rectification and erasure

The GDPR includes a right for individuals to request that inaccurate personal data be rectified or completed if it is incomplete and on receipt of such a request, we will respond within one calendar month.

Document	Authorised by	Issue/ Rev	Date	Page
EWG-Q-P-04 – Data Protection Policy	EDB	1b	Sept 2019	6 of 7



It also includes a right in certain circumstances to have personal data erased and on receipt of such a request made verbally or in writing we will respond within one month.

9. Disclosure and Sharing of Personal Information

In certain circumstances, the law allows personal data to be disclosed to law enforcement agencies without the consent of the individual concerned. Under these circumstances the Group will disclose requested data. We will however ensure that the request is legitimate seeking legal advice where necessary.

Personal data may be shared with any entity within the Group.

We may also disclose personal data to third parties in order to enforce or apply any contract with the data subject, or to protect our rights, property or safety of our employees, customers, suppliers or visitors. This includes exchanging information with other organisations for the purposes of fraud protection or credit risk reduction.

10. Training

The Group will provide training to all employees who handle personal data to help them to understand their responsibilities when handling data.

11. Data Storage

Personal Data must be processed securely by means of appropriate technical and organisational measures.

The measures we take ensure the confidentiality integrity and availability of our systems and services and the personal data we process within them

Data which is stored electronically is protected from unauthorised access, accidental deletion and malicious hacking attempts with password protection and encryption (where appropriate).

Personal Data stored on paper is kept in a secure place and when being used should not be left where unauthorised people can see it.

All servers and computers containing data is protected by approved security software and a firewall.

12. How to Complain

If you are unhappy with the way we hold your information or deal with your request to access it you have the right to lodge a complaint with the Information Commissioner who is the supervisory authority for the United Kingdom and may be contacted at <https://ico.org.uk/concerns> or by telephone on 0303 123 1113.

Document	Authorised by	Issue/ Rev	Date	Page
EWG-Q-P-04 – Data Protection Policy	EDB	1b	Sept 2019	7 of 7