25 May 2018

THE WORSHIPFUL COMPANY OF WHEELWRIGHTS

Data Protection Policy

Contents

This policy covers the following:

1. Background

In the course of running its day to day business and promoting its charitable and educational aims, The Worshipful Company of Wheelwrights (the '**Company**'), may collect and process information about its members and staff as well as members of the public such as enquirers and correspondents. The use of such information ('**personal data',** as explained in more detail below) is regulated by data protection law (the '**Data Protection Legislation**', explained below). This policy sets out how the Company intends to comply with the key rules that apply to the processing of personal data in the United Kingdom.

Description of the Company's processing activities

The Company regularly processes the following categories of personal data:

Staff: The Company has a small number of employees, about whom it holds personal data such as employment history, education and qualifications, and identifiers such as contact details and record of employment with the Company. Very occasionally, the Company may process information about its employees' health or medical details. The Company processes such employee personal data for ordinary staff administration purposes, including salary payment and conferring other benefits, conducting appraisals, training and management. It also collects personal data about prospective candidates in the recruitment process. The Company holds some information about its employees and former employees for archival and historical research purposes, for example, to maintain a roll of past Masters and Clerks.

Members: The Company holds the personal data of its past, present and prospective members (Liverymen, Freemen, Yeomen, Journeymen and Apprentices). The personal data held includes members' education and employment history, qualifications, personal and family circumstances, as well as financial and contact details. The Company processes such personal data in order to administer membership, to organise events such as meetings and fellowship events, and to collect subscription fees. It may also process members' personal data for fundraising purposes including seeking endowments such as gifts, trusts and bequests. The Company holds some information about its members for archival and historical research purposes, for example, to maintain a roll of past Freemen and Liverymen which may be drawn on in response to public enquiries relating to genealogical research.

Guests: The Company retains a list of the names of its guests and those of Company members attending events, for the organisation of events and the information of other attendees at the same event and thereafter for consultation in connection with applications for the Freedom and Livery for which prior attendance as a guest at events is required.

Beneficiaries: The Company's charitable and educational activities have been a fundamental objective throughout its history. In order to further its charitable and educational aims, the Company may process personal data about beneficiaries, including award and prize winners, and potential beneficiaries, which may include personal, family and financial circumstances, education, and employment history. The Company may occasionally process information about beneficiaries' or prospective beneficiaries' health or medical details. The Company may also process personal data about its beneficiaries for historical and archiving purposes.

The public: The Company may enter into correspondence with members of the public, such as enquirers, and correspondents. When it does so, the Company may collect incidental personal data such as contact details and personal circumstances, and processes such personal data in order to respond to queries and deal with ad hoc issues. Also in the case of working wheelwrights in the UK and overseas to use such personal information to inform them about events/initiatives of the Company and its associated Charity.

Suppliers: The Company processes personal data concerning its suppliers of goods and services, including identifiers such as contact details, financial information and purchase history. The Company processes such information in order to purchase goods and services, to pay its suppliers and to maintain its accounts and records. .

This policy does not document every part of the Data Protection Legislation which may be relevant, but merely focuses on the key aspects that are likely to be applicable to the Company. Should other issues arise in practice not covered by this policy, the Company will consider these separately at the time. The Company will review this policy annually, and may amend it from time to time as it sees fit.

2. Applicable data protection law

Data protection law in England and Wales is primarily found in the General Data Protection Regulation ('**GDPR**'). supplemented by the Data Protection Act 2017. In this policy, any reference to the Data Protection Legislation means the GDPR, as supplemented by the Data Protection Act 2017 ('**DPA 17**'), whichever is in force at the time.

Data Protection Legislation is enforced in England by the Information Commissioner, operating through the Information Commissioner's Office (the '**ICO**'). The ICO has a broad range of powers including the ability to issue fines.

3. Key concepts of applicable data protection law

The Data Protection Legislation relies on a number of key definitions, which are explained below.

'***personal data***' means any information relating to an identified or identifiable natural person (a 'data subject', which is explained in more detail below). An identifiable natural person is one who

can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the identity of that natural person.

The Company will hold personal data about its past, present and prospective members (including Liverymen and Freemen) staff and members of the public such as beneficiaries and job applicants, as well as its suppliers. The Company may hold such personal data both in electronic and hard copy format, in records, correspondence and minutes.

'***processing***' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaption or alteration, retrieval consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing is interpreted very broadly, so that almost all activities organisations carry out in relation to their personal data are captured by the definition.

The Company will generally be deemed to be processing any personal data that it may collect, record, store and/or disclose.

'***controller***' means the natural or legal person, public authority, agency or other body, which determines the purposes and means of the processing of personal data. The Data Protection Legislation applies to controllers, who must comply with its requirements.

The Company will generally be a controller in relation to the personal data of its members, staff, members of the public such as beneficiaries and enquirers, and suppliers.

'***processor***' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. Where a controller uses a processor to process personal data on its behalf, the controller must only use a processor that provides sufficient guarantees to ensure that personal data is processed securely, and in accordance with the requirements of the GDPR. Controllers must engage processors by way of a contract incorporating the provisions specified by Article 28 of the GDPR.

The Company may use processors for a variety of purposes; for instance, to store personal data, to send email communications, or to calculate staff payroll. In each case, it must have conducted sufficient due diligence to be able to evaluate whether the processor offers sufficient guarantees to protect personal data and must ensure that the processor is bound by a contract that incorporates the provisions specified by the GDPR. The requirements around appointing processors are explained in more detail below (see Section 7, below).

'***special categories of personal data***' means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic or biometric data, data concerning health (including medical data, and medical records, for example), or concerning an individual's sex life or sexual orientation. Special categories of personal data the company will collect will be to meet its health and safety obligations regarding dietary and medical information and information relating to the health of members received by the Clerk or other Officers which might be passed to the Almoner and Chaplain.

The special categories of personal data require a higher standard of care. If a personal data breach (as defined below) occurs that involves the loss of any of the special categories of personal data, the ICO will regard this as a serious breach. The GDPR also requires that personal data relating to criminal convictions and offences is treated with a higher standard of care.

The Company is generally unlikely to hold a significant volume of the special categories of personal data, though in the event that it does, it must ensure the information is handled accordingly.

'***data subject***' means an individual to whom personal data relate. Typically, these are employees, customers, and suppliers.

The categories of data subject, whose personal data the Company is likely to process, will include members, staff, suppliers, beneficiaries and members of the public.

'***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.

A personal data breach may be accidental, such as a system failure, or loss of an electronic or physical file, or malicious, such as a cyberattack. In the event that the Company suffers a personal data breach, it must take specific steps, explained below in this policy.

4. The data protection principles

The data protection principles are standards which the Company must observe when processing personal data. These principles are as follows:

i. Fairness, lawfulness and transparency

Fairness: Organisations generally cannot process individuals' personal data in a way that an individual would not have reasonably expected. Collecting personal data on the pretext of one purpose and then using it for another, unrelated purpose is unlikely to be fair. The Company will consider whether its uses of personal data would fall within the reasonable expectations of the affected data subjects.

Transparency: Organisations must provide certain prescribed information to individuals when processing their personal data, including the organisation's identity, the purposes for which personal data are being processed, or are to be processed, and any third party recipients of the personal data. The transparency information must accurately reflect the controller's use of personal data. The Company provides this by way of a privacy notice.

The Company must ensure that its privacy notice, and any other means by which it makes the transparency information available to data subjects (such as a disclaimer on a paper form) accurately and comprehensively reflects its processing activities.

Lawfulness: Organisations must establish at least one of a number of lawful grounds for processing. These lawful grounds are set out in Article 6 of the GDPR and are as follows:

1) Processing is necessary for the purposes of **legitimate interests** pursued by the controller or by a third party except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require the protection of personal data.

2) Processing is necessary for the **performance of a contract** to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract.

3) Processing is necessary for **compliance with a legal obligation** to which the controller is subject.

4) Processing is necessary in order to protect the **vital interests of the data subject** or of another person.

5) Processing is necessary for the performance of a task carried out in the **public interest** or in the exercise of official authority vested in the controller.

6) The data subject has given his or her **consent** to the processing. Note that to be valid, consent must be freely-given, informed (by way of the transparency notice, explained above) specific, and capable of withdrawal at any time, without detriment to the data subject. Consent must be indicated by way of an unambiguous, positive affirmation by the data subject. Consent cannot be inferred from the absence of an objection and will not be valid where the data subject does not have a genuine choice.

In practice, the Company will frequently be able to rely on the first and second grounds, (the legitimate interests ground and performance of a contract) for many of its activities. Note that the grounds for processing the special categories of personal data are different.

ii. Purpose limitation

This principle requires that the purposes for which personal data are processed are limited to those purposes specified in the transparency information that has been provided to the affected data subjects, and not processed for any further, incompatible purposes. Note that any further processing operations for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes are not considered to be incompatible purposes.

The Company will only process personal data it holds for those purposes specified in the website privacy notice, or other such transparency notice.

iii. Data minimisation

Personal data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

The Company will only collect the personal data that is strictly necessary for the purpose for which it was collected, and will not collect additional, unnecessary personal data on a 'just in case' basis.

iv. Accuracy

Personal data must be kept accurate, and up to date.

The Company must ensure that any requests from data subjects to update their personal data are dealt with promptly, having satisfied itself as to the requester's identity.

v. Storage limitation

Personal data must not be kept for longer than is necessary for the purposes for which the data are processed. The duration for which personal data are stored will be dictated by applicable legal, business or other reasons, such as retention periods driven by tax legislation.

If the Company cannot establish a valid legal, business or other reason for retaining personal data, it should be securely deleted. The Company will specify the periods for which personal data are stored in a record retention policy. After the storage period has expired, personal data will be deleted.

Note that the Company may store some categories of personal data for longer periods where such processing is solely for archiving purposes in the public interest, or historical research purposes. In such cases, the Company must implement appropriate safeguards, such as allowing data subjects to request deletion of some of their personal data.

vi. Integrity and confidentiality

Personal data must be processed in a manner that ensures its security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The Company will take appropriate measures that are proportionate to the risk associated with the personal data it holds. Such measures may be technical, such as encryption and password protection of electronic devices and electronic storage media (e.g. USB drives), or organisational, for example, by operating a layered access policy, appropriate vetting of staff who have access to personal data, conducting appropriate due diligence on any third parties that process personal data on the Company's behalf, and binding them by an appropriate engagement contract. The Company will consider regularly reviewing and testing its security measures.

vii. Accountability

Controllers are responsible for compliance with the principles explained above, and must be able to demonstrate compliance through its data protection policy, documented data protection reviews and record of data protection training.

5. Data subjects' rights

Data Protection Legislation confers a number of rights upon data subjects, which controllers must observe. Data subjects' rights are a cornerstone of the Data Protection Legislation and must be dealt with promptly should one arise. The Company is unlikely to receive data subject requests on a regular basis so this Policy does not go into detail, but the Company must be able to recognise a request from a data subject to exercise his or her rights, should one arise. The most relevant of these rights, from the Company's perspective, are summarised below:

i. Data subject access requests

Data subjects are entitled to access their personal data held by the Company on request (Article 15 GDPR). The response to a data subject access request must include certain information, such as: the purposes of the processing; the recipients (or categories of recipient) to whom the personal data have or will be disclosed; and individuals' rights to have their data corrected, deleted or to restrict the processing of their data.

Note that under the GDPR, the information must be provided to data subjects free of charge and within one month of the request.

ii. The right to be forgotten

Data subjects have the right to request the Company erase all data held in respect of them in various circumstances (Article 17 GDPR). However, the right to be forgotten is not an absolute right, and the Company is only obliged to give effect to a request in a number of specific situations, the most relevant of which are likely to be:

1) Where the purpose for which the personal data were processed no longer applies; or

2) Where the Company's processing of the personal data is based on consent and the data subject withdraws his or her consent.

iii. The right to rectification

Data subjects have the right to have incorrect personal data about them corrected without undue delay (Article 16 GDPR).

The Company must endeavour to ensure that any personal data it processes is up to date and correct. Where an error or inaccuracy is discovered, the Company should correct this as soon as possible.

iv. The right to data portability

Data subjects have the right, in certain circumstances, to access their data in machine-readable format and, where technically possible, to have their data transferred directly from the Company to another data controller (Article 20 GDPR). However, the circumstances in which the right to data portability arises are limited and, at present, seem unlikely to be relevant to the Company.

v. The right to object

Data subjects have the right, in a number of specific circumstances, to object to having their personal data processed (Article 21 GDPR). The most relevant of these circumstances are where the processing is based on the Company's legitimate interests (explained in section 4(i)(1) above). Data subjects may also object to their personal data being processed by the Company for direct marketing purposes.

6. Other requirements

The Company must process personal data in accordance with the principles explained above. However, the Data Protection Legislation imposes a number of additional requirements, which are explained below.

i. Breach notification

The Company has a documented data protection breach management plan in place. It is noted in the event of a data protection breach, the ICO would regard the absence of a breach management plan as an aggravating factor.

Reporting breaches to the ICO

Under the GDPR, if a data security breach occurs, the Company (as controller) must notify the breach to the ICO "*without undue delay" and, where feasible, within 72hrs of the personal data breach occurring*." However, this notification requirement does not apply where the breach "*is unlikely to result in a risk to the rights and freedoms*" of the individuals concerned.

The notification must include the information specified in Article 33(3) of the GDPR, and where it is not possible to provide all the information at once, it may be provided in phases.

Reporting breaches to individuals

Where a data security breach occurs, and it is likely to result in a "high risk" to the rights and freedoms of the individuals concerned, the Company must notify the affected individuals *"without undue delay".* Article 34(2) of the GDPR specifies what information must be provided. However, the Company is not required to notify data subjects if:

1) The personal data concerned had been rendered unintelligible (for example, by way of encryption); or

2) Subsequent measures have been taken by the Company so that there is no longer a high risk to the individuals; or

3) It would involve disproportionate effect to communicate to each affected data subject individually, although where this applies then a general public communication must be made.

The Company must maintain a schedule of data breaches (whether or not notification was made at the time), to comply with Article 33(5) of the GDPR.

ii. Data protection impact assessments (DPIAs)

A DPIA consists of a documented consideration and evaluation of the data protection risks arising from a proposed new processing activity, along with recommended mitigation strategies to address the risks.

Under Article 35 of the GDPR, the Company is required to undertake a DPIA "*where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons*"

The Company does not believe that the nature of its processing is such that there is likely to be a high risk to the rights and freedoms of the data subjects whose personal data it holds. As a result, the Company does not believe that it is necessary for it to undertake any DPIAs.

The Company will keep this conclusion under review, including any guidance issued from ICO, or practice in other similar organisations.

7. Third party processors

The rules around the appointment of processors (the meaning of which is explained in Section 3, above) are strict, and amount to an organisational security measure. In the event that the Company were to suffer a personal data breach involving a third party processor, the ICO would expect to see that appropriate due diligence had been conducted on that provider and that the appropriate contract was in place.

The Company will ensure that it has a written contract which meets the requirements of GDPR in place with each processor it uses. The Company will only use processors that guarantee they will meet the requirements of the GDPR and will protect data subjects' rights.

Before engaging a processor, the Company will check that the processor has appropriate technical and organisational measures in place to keep data secure; and that the processor's staff who will be engaged in processing personal data on behalf of the Company are subject to a duty of confidentiality and receive regular training in data protection matters.

The Company will regularly review the activities and processes of any processors it uses, to check that the processor is processing personal data in line with its internal processes; complying with relevant requirements under the Data Protection Legislation and its contractual commitments in respect of the personal data. The Company will ensure that its contract with each processor contains provisions concerning sub-contracting which meet the requirements of GDPR.

8. Further information

For further information about this policy, and the Company's data handling practices, please contact:

Mrs Susie Morris
clerk@wheelwrights.org
020 8673 4820
The Worshipful Company of Wheelwrights
90 Fernside Road
London
SW12 8LJ

THE WORSHIPFUL COMPANY OF WHEELWRIGHTS' GROUP DATA PROTECTION PRIVACY NOTICE

General Data Protection Regulations (EU 2016/679)

INTRODUCTION

1. The Wheelwrights' Company Group is committed to keeping your personal information secure and private. This privacy notice lets you know what why we collect personal data, how we use it and the legal basis on which the information is held.
2. The Company's Data Protection Policy Document, which provides more detail on the applicable data protection law, principles and data subject rights, is available on request and to members on the Company's website.

THE GROUP

3. The Wheelwrights' Company Group, in the context of this Privacy Notice and to which the Group's data protection policy applies, is defined as The Worshipful Company of Wheelwrights (The Company) and the Wheelwrights' Charity (The Charity)

DATA CONTROLLER AND DATA PROTECTION OFFICER

4. The Wheelwrights' Company is the Data Controller, the organisation responsible for the accuracy and safeguarding of the data.

5. Due to the small size of the Company and the Charity no Data Protection Officer is nominated.

THE PURPOSE AND BASIS FOR PROCESSING YOUR PERSONAL DATA

6. We collect, use and store personal data for our legitimate business interest or compliance with legal obligations. In order to be able to conduct our business, the Group needs to collect certain personal data which is necessary to fulfil the functions, responsibilities and activities expected of the Group. Personal data, as required, is collected about our Liverymen, Freemen, Yeomen and Journeymen (collectively members) our staff, working wheelwrights, members of the public and suppliers with whom we have contact so that we can:

- Maintain a database of names, addresses, email addresses, telephone numbers of all those with whom we need to communicate to pursue the activities of the Group including Company fellowship events.
- Communicate to our members, staff, fellow livery organisations, working wheelwrights, suppliers and beneficiaries, as appropriate, news of our activities and future plans, including fundraising for the Charity.

- Understand the knowledge, experience, interests and professional qualifications of members in order to populate adequately our committees, sports teams and other activities requiring membership participation.
- Meet the needs of our contacts and suppliers and their requirements, to send documents and information about Company matters.
- In the case of officers and staff of the Company or the Charity, manage contracts and relationships with third party service providers and professional advisers.
- Fulfil the responsibilities and obligations of the livery to the Corporation of the City of London with respect to the election of Sheriffs and the Lord Mayor. This includes publishing the names and addresses of liverymen in The City of London Directory, Livery Companies Guide (the Blue Book), the City of London White Book and the Electoral Role for election of the Lord Mayor and Sheriffs.
- Understand the competences and suitability of job applicants.
- Maintain a list of donors to the Charity, for the purpose of claiming Gift Aid on their donations

7. It is the Group's view that holding and maintaining the above information is necessary to conduct its business efficiently in the interests of the Company, its members, the Charity and those with whom we have contact. Information will be retained on members indefinitely for historical records. Information required by statue or law will be retained in accordance with the legal requirements. Information held, in order to carry out the legitimate business of the Group will be retained for the period necessary to be able to conduct the business effectively.

NATURE OF THE INFORMATION HELD

8. Personal information is defined as anything that can identify a living person (NB: the regulations do not cover the deceased and thus by far the greater part of our archives do not come under these regulations).

9. The information we collect consists primarily of information submitted by members on their Freedom/Livery Application Form and accompanying CV and updates members have sent us, as well as banking information e.g. on Standing Order forms for the Charity. This may include:

- Names and addresses
- Telephone numbers and email addresses
- Age and gender
- Names, age and gender of partners and family members
- Photographs
- Professional qualifications
- Interests
- Employment
- Charity Standing Orders and Gift Aid Declarations
- Dietary requirements (for those attending dinners – legal health and safety requirement)
- Medical Conditions (only if volunteered by the data subject to assist the Company in fulfilling its welfare and health and safety obligations)

SHARING AND TRANSFER OF DATA

10. The Clerk (which may include any assistant) is the principal processor of your personal data. The Company's officers, Trustees of the Charity and, in respect of membership applications, the Court may also look at personal data from time to time. The Group may also share personal data with third parties for the purposes listed above including venues for certain fellowship functions, who might require a list of attenders for security and practical purposes, HMRC in order to process a claim for gift aid on donations to the charity and the operators of our staff payroll.

The Company has no intention of knowingly transferring your data outside the EU but recognises that certain service providers such as banks and investment managers who hold personal data relating to officers and staff of the Company may process personal information outside the UK. We will seek their assurance that it is secure and protected from unauthorised access. The Group does not carry out automated decisions using technology including profiling.

11. Members of the Company need to give their clear permission for their personal data to be shared with other members. Members of the public, namely working wheelwrights will need to give their clear permission for their personal data to be shared with members of the Company and shown on the public part of the Company website. Liverymen and Freemen of the Company will be asked specifically whether they wish their personal data, held on the Company's database, to be shared with other members. Similarly working wheelwrights will be asked specifically whether they wish their personal data, held on the Company's data base, to be shared with members of the Company and appear on the public part of the Company website. Not responding to this request will be interpreted as declining the sharing of personal information.

YOUR RIGHTS

12. All individuals have the right to be informed about the processing of their personal data, which this privacy notice sets out to do, the right to have their data corrected if inaccurate, the right to object to or restrict processing, the right to erase data held and the right to access their personal data.

Further information

For further information about this Privacy Notice, the Policy and the Company's data handling practices, please contact::

Mrs Susie Morris
clerk@wheelwrights.org
020 8673 4820
The Worshipful Company of Wheelwrights
90 Fernside Road
London
SW12 8LJ

25th May 2018

Appendix 2 to Wheelwrights' Company
Data Protection Policy

DATA SUBJECT ACCESS REQUEST PROCEDURE

Introduction

1. The GDPR (General Data Protection Regulation) creates certain rights for Data Subjects. The Wheelwrights' Company must be able to comply with these rights. The GDPR provides the following rights for individuals:

- Right of Access (also known as a Subject Access Request) (such requests must be dealt with within 1 calendar month)
- Right to Rectification (under GDPR must be dealt with without undue delay)
- Right to Erasure (under GDPR must be dealt with without undue delay)
- Right to Restrict Processing
- Right to Data Portability
- Right to Object
- Right in relation to automatic decision making and profiling

It should be noted that Data Subjects can make such requests verbally, for example, over the telephone, as well as in an email or postal letter.

Purpose

2. The purpose of this guide is to provide a procedure to follow when a data subject request is received by the Company,

Responsibilities

3. All officers and staff have a responsibility to recognise a request and to comply with the procedure as follows. The Company does not have a nominated Data Protection Officer but the Clerk is designated the Data Protection Champion.

Procedure

4.1 Annex A to this appendix is a Data Subject Access Request Form which should be completed for a data subject requesting information.
4.2 Where a request is received by officers or staff covering any of the GDPR Data Subject Rights the request must be passed to the Clerk immediately.
4.3 The Clerk will arrange for the request to be processed and a response made to the Data Subject in line.

Requirements

5. Whilst Data subjects have a 'right' to seek personal information, some essential safeguards and criteria have to met. The following list is to be followed before release of any personal information:

a. Confirm identity of person making request (Annex A to be completed).

b. Confirm entitlement to the data.
c. Check nature of information being requested and where that data will be held as:
    i. Financial – Clerk, Honorary Treasurer, JCA Chartered Accountants
    ii. Personal information regarding family, interests, professions etc; Company Data Base – Clerk, Archivist
    iii. Personal data regarding Livery Company: Clerk, Master
    iv. Information regarding the charity: Chairman of Charity Trustees
    v. Information regarding working wheelwrights, as members of the public: Chairman of the Craft Committee or his/her nominated representative
d. Clerk to verify and agree response.

June 2018

Annex A to Appendix 2

SUBJECT ACCESS REQUEST FORM

You should complete this form if you want us to provide you with a copy of any personal data we hold about you. You are entitled to receive this information under EU General Data Protection Regulation (GDPR), which was effective from 25 May 2018. We will also provide you with information about any processing of your personal data that is being carried out, the retention periods which apply to your personal data, and any rights to rectification, erasure, or restriction of processing that may exist. You have a right to complain to the Information Commissioner's Office should you be unhappy about the way we process your data.

We will endeavour to respond promptly and in any event within one month of the latest of the following:

- Our receipt of your written request; or
- Our receipt of any further information we may ask you to provide to enable us to comply with your request.

The information you supply in this form will only be used for the purposes of identifying the personal data you are requesting and responding to your request. You are not obliged to complete this form to make a request, but doing so will make it easier for us to process your request quickly.

SECTION 1: Details of the person requesting information

Full name:	
Address:	
Contact telephone number:	
Email address:	

SECTION 2: Are you the data subject?
Please tick the appropriate box and read the instructions which follow it.

☐ **YES**: I am the data subject. I enclose proof of my identity (see below).
(please go to section 4)

☐ **NO**: I am acting on behalf of the data subject. I have enclosed the data subject's written authority and proof of the data subject's identity and my own identity (see below).
(please go to section 3)

To ensure we are releasing data to the right person we require you to provide us with proof of your identity and of your address. Please supply us with a photocopy or scanned image (do not send the originals) of one of both of the following:

1) Proof of Identity:
   Passport, photo driving licence, national identity card, birth certificate.

2) Proof of Address
   Utility bill, bank statement, credit card statement (no more than 3 months old); current driving licence; current TV licence; local authority tax bill, HMRC tax document (no more than 1 year old).

If we are not satisfied that you are who you claim to be, we reserve the right to refuse to grant your request.

SECTION 3
Details of the data subject (if different from section 1)

Full name:	
Address:	
Contact telephone number:	
Email address:	

SECTION 4: What information are you seeking?
Please describe the information you are seeking. Please provide any relevant details you think will help us to identify the information you require.

Please note that if the information you request reveals details directly or indirectly about another person we will have to seek the consent of that person before we can let you see that information. In certain circumstances, where disclosure would adversely affect the rights and freedoms of others, we may not be able to disclose the information to you, in which case you will be informed promptly and given full reasons for that decision.

While in most cases we will be happy to provide you with copies of the information you request, we nevertheless reserve the right, in accordance with Article 12 of the GDPR to charge a fee or refuse the request if it is considered to be "manifestly unfounded or excessive". We will, however, make every effort to provide you with a satisfactory form of access or summary of information if suitable.

SECTION 5: Information about the collection and processing of data

If you want information about any of the following, please tick the boxes:

- Why we are processing your personal data ☐
- To whom your personal data are disclosed ☐
- The source of your personal data ☐
- How long we retain your data ☐

SECTION 6: Declaration

Please note that any attempt to mislead may result in prosecution.

I confirm that I have read and understood the terms of this subject access request form and certify that the information given in this application. I understand that it is necessary to confirm my / the data subject's identity and it may be necessary to obtain more detailed information in order to locate the correct personal data.

Signed…… **Date** ……..

Documents which must accompany this application:

- **Evidence of your identity (see section 2)**
- **Evidence of the data subject's identity (if different from above)**
- **Authorisation from the data subject to act on their behalf (if applicable)**

Please return the completed form to:
The Clerk
The Worshipful Company of Wheelwrights
90 Fernside Road
London
SW12 8LJ

Email: clerk@wheelwrights.org
Tel: 020 8673 4820

Correcting Information

If after you have received the information you have requested you believe that:

- the information is inaccurate or out of date; or
- we should no longer be holding that information; or
- we are using your information for a purpose of which you were unaware;
- we may have passed inaccurate information about you to someone else;

then you should notify the Clerk at once.

May 2018

Appendix 3 to Wheelwrights'
Company Data Protection Policy

DATA PROTECTION BREACH MANAGEMENT PLAN

Occasions for reporting a data security breach

1. The ICO must be informed if a data security breach occurs, "*without undue delay" and, where feasible, within 72hrs of the personal data breach occurring*." However, this notification requirement does not apply where the breach "*is unlikely to result in a risk to the rights and freedoms*" of the individuals concerned. The notification must include the information specified in Article 33(3) of the GDPR, and where it is not possible to provide all the information at once, it may be provided in phases.

2. Where a data security breach occurs, and it is likely to result in a "high risk" to the rights and freedoms of the individuals concerned, the Company must notify the affected individuals "without undue delay". Article 34(2) of the GDPR specifies what information must be provided. However, the Company is not required to notify data subjects if:

a) The personal data concerned had been rendered unintelligible (for example, by way of encryption); or

b) Subsequent measures have been taken by the Company so that there is no longer a high risk to the individuals; or

c) It would involve disproportionate effect to communicate to each affected data subject individually, although where this applies then a general public communication must be made.

Action to be taken in the event of a data security breach

3. The following procedure is to be followed in the event of a data security breach being identified:

a. Identify and assess the nature of the information that has been released including if possible, date and time of the breach and recipients of the unauthorised personal data information.
b. Make a risk assessment of the severity of the breach in accordance with the criteria at paragraphs 1 and 2 above.
c. Depending on the outcome of (b), decide whether a report is required to the ICO and/or individual data subjects.
d. If the breach is assessed to have occurred as a result of criminal activity, inform the police.
e. Report the breach to the Clerk and the Master.
f. Ascertain how/why the breach occurred.
g. Inform and liaise with Rosco Solutions (01245 474145) and/or Westwood Associates (01753 887161) as appropriate to implement immediate remedial measures to prevent further breaches.
h. Implement other immediate changes to other security measures (locks, access, passwords etc) as appropriate and as advised by IT consultants, including informing all staff of the breach.
i. Instigate longer term damage assessment
j. Implement longer term changes to security measures
k. Record the breach in the Data Security Breach log. (Article 33(5) of the GDPR).

DATA PROTECTION - APPROACH TO FUNDRAISING

Introduction

1. The Wheelwrights' Company is not primarily a fundraising body. Nevertheless, from time to time the Company may deem it appropriate to raise funds for its charity. In any case, it is the Company's declared policy that all members should consider making regular voluntary donations to the Company's charity and as such, reminders of this will be made from time to time to members.

2. For the most part, approaches made to data subjects regarding fundraising will only be made with those with whom the company already has an established relationship. On this basis the Company believes it has a legitimate interest in holding research information and making such approaches.

Fundraising relationships

3. The Company may wish to form fundraising relationships with the following categories of data subjects:

a. Members of the Wheelwrights' Company and their immediate families
b. Senior members of industries that have a common interest in disability
c. Senior members of companies the company has an established business relationship with including consultants, suppliers of equipment and services or other philanthropic organisations with common interests

Methods of contact

4. The Company may employ one or more of the following methods of communications:

a. Members: email, letter, newsletter, on the basis that there is an established relationship and the Company's expectations of its membership
b. Senior members of Industry and Private Individuals: Normally via a personal referral and contact and initial contact made by letter followed up by emails as agreed.
c. Other Companies and organisations: To a business address by letter explaining the common interest

Telephone preference scheme (TPS) and fundraising preference scheme (FPS)

5. The Company is aware of the TPS, the Mail Preference Service and FPS and will refer to these registers before making any unsolicited approaches.

Reasons for holding personal data for fundraising

6. The Company may wish to hold certain personal data information for the following reasons:

a) We want to maintain a list of people who have donated to us before, so that we can contact them to ask them to do so again

b) We want to maintain a list of people who have explicitly told us that they don't want to contact us again
c) We want to use (a) to research the donors' financial background using public sources to work out what kind of approach to make to them
e) We want to claim gift aid on a person's donations
f) We want to keep their information up to date

7. This data will not be shared with any organisation outside of the Wheelwrights' Company Group.

June 2018