IADA Limited

Controlled Document

Document Name:	**Data Protection Policy**
Review Schedule	Every two years
Next review due	April 2020
Owner (Responsibility)	Mike Casson, Non-Executive Chairman
Pass amendments to:	IADA Administrator
Revision History	See appendix
Document Location	City Seals & Bearings Office

Document Description

This document outlines our legal requirements under the General Data Protection Regulations and the processes for how IADA Limited meets them. Note: until GDPR come into force on 25 May 2018 the current Data Protection Act 2000 will continue to apply.

Implementation and Quality Assurance

Implementation is immediate and this Policy shall stay in force until any alterations are formally agreed.

The Policy will be reviewed every two years by the Non-Executive Chairman, sooner if legislation, best practice or other circumstances indicate this is necessary.

All aspects of this Policy shall be open to review at any time. If you have any comments or suggestions on the content of this policy please contact admin@iadaltd.co.uk or at IADA Limited, 23-25 Stevenson Street, Sheffield, S9 3XG, 0114 2436143

Data Protection Policy

Introduction

The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the European Council and the European Commission intend to strengthen and unify data protection for individuals within the European Union (EU). It also addresses the export of personal data outside the EU. The primary objectives of the GDPR are to give citizens back control of their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. When the GDPR takes effect it will replace the data protection directive (officially Directive 95/46/EC) from 1995. The regulation was adopted on 27 April 2016 and applies from 25 May 2018 after a two-year transition period.

The 1998 Data Protection Act, which came into force on 1 March 2000, will continue to apply until the new General Data Protection Regulations come into force in May 2018.

The following guidance is not a definitive statement on the Regulations, but seeks to interpret relevant points where they affect IADA Limited.

The Regulations cover both written and computerised information and the individual's right to see such records.

It is important to note that the Regulations also cover records relating to staff and customers.

All IADA Limited staff are required to follow this Data Protection Policy at all times.

The Non-Executive Chairman has overall responsibility for data protection within IADA Limited but each individual processing data is acting on the controller's behalf and therefore has a legal obligation to adhere to the Regulations.

Definitions

Processing of information – how information is held and managed.
Information Commissioner - formerly known as the Data Protection Commissioner.
Notification – formerly known as Registration.
Data Subject – used to denote an individual about whom data is held.
Data Controller – used to denote the entity with overall responsibility for data collection and management. IADA Limited is the Data Controller for the purposes of the Act.
Data Processor – an individual handling or processing data
Personal data – any information which enables a person to be identified
Special categories of personal data – information under the Regulations which requires the individual's explicit consent for it to be held by the company.

Data Protection Principles

As data controller, IADA Limited is required to comply with the principles of good information handling.

These principles require the Data Controller to:

1. Process personal data **fairly**, **lawfully and in a transparent manner.**
2. Obtain personal data only for one or more **specified** and **lawful purposes** and to ensure that such data is not processed in a manner that is incompatible with the purpose or purposes for which it was obtained.
3. Ensure that personal data is **adequate**, **relevant and not excessive** for the purpose or purposes for which it is held.
4. Ensure that personal data is **accurate** and, where necessary, **kept up-to-date.**
5. Ensure that personal data is not kept for any longer than is necessary for the purpose for which it was obtained.
6. Ensure that personal data is kept secure.
7. Ensure that personal data is not transferred to a country outside the European Economic Area unless the country to which it is sent ensures an adequate level of protection for the rights (in relation to the information) of the individuals to whom the personal data relates.

Consent

IADA Limited must record service users' explicit consent to storing certain information (known as 'personal data' or 'special categories of personal data') on file.

For the purposes of the Regulations, personal and special categories of personal data covers information relating to:

1. Name and contacts details.
2. Online identifiers such as an IP address & emailed addresses.
3. Payment information, bank details etc.
4. Whether he/she is a member of a trade union.
5. Any modified medical requirements.
6. Any Health & Safety assessments.
7. Any other special categories

As a general rule IADA Limited will always seek consent where personal or special categories of personal information is to be held.

It should also be noted that where it is not reasonable to obtain consent at the time data is first recorded and the case remains open, retrospective consent should be sought at the earliest appropriate opportunity.

Obtaining Consent

Consent may be obtained in a number of ways depending on the nature of the records that need to be kept, and consent must be recorded on or maintained with the records:

- face-to-face
- written
- telephone
- email.

Face-to-face/written

A pro-forma should be used.

Telephone

Verbal consent should be sought and noted on the record.

E-mail

The initial response should seek consent.

Consent obtained for one purpose cannot automatically be applied to all uses e.g. where consent has been obtained from a customer in relation to information needed for the provision of a service, separate consent would be required if, for example, direct marketing were to be undertaken.

Preliminary verbal consent should be sought at point of initial contact as personal and/or special categories of personal data will need to be recorded either in an email or on a computerised record. The verbal consent is to be recorded in the appropriate fields on the computer record or stated in the email for future reference. Although written consent is the optimum, verbal consent is the minimum requirement.

Specific consent for use of any photographs and/or videos taken should be obtained in writing. Such media could be used for, but not limited to, publicity material, press releases, social media, and website. Consent should also indicate whether agreement has been given to their name being published in any associated publicity. If the subject is less than 18 years of age then parental/guardian consent should be sought.

Individuals have a right to withdraw consent at any time.

Ensuring the Security of Personal Information

Unlawful disclosure of personal information

1. It is an offence to disclose personal information ‘knowingly and recklessly’ to third parties.

2. A customer’s individual consent to share information should always be checked before disclosing personal information to another agency/supplier.

3. Where such consent does not exist information may only be disclosed if it is in connection with criminal proceedings or in order to prevent substantial risk to the individual concerned. In either case permission of the Non-Executve Chairman should first be sought.

4. Personal information should only be communicated within IADA Limited's staff on a strict need to know basis. Care should be taken that conversations containing personal or special categories of personal information may not be overheard by people who should not have access to such information.

Ethnic Monitoring

In order for IADA Limited to monitor how well our staff, customers and suppliers reflect the diversity of the local community we may request that they complete an Equality and Diversity Monitoring form. The completion of the form is voluntary, although strongly encouraged. Responses are securely stored and held on a pass worded database for statistical purposes.

Use of Files, Books and Paper Records

In order to prevent unauthorised access or accidental loss or damage to personal information, it is important that care is taken to protect personal data. Paper records should be kept in locked cabinets/drawers overnight and care should be taken that personal and special categories of personal information is not left unattended and in clear view during the working the day. If your work involves you having personal / and/or special categories of personal data at home or in your car, the same care needs to be taken.

Disposal of Scrap Paper, Printing or Photocopying Overruns

Be aware that names/addresses/phone numbers and other information written on scrap paper are also considered to be confidential. Please do not keep or use any scrap paper that contains personal information but ensure that it is shredded.

If you are transferring papers from your home, to the office for shredding this should be done as soon as possible and not left in a car for a period of time. When transporting documents they should be carried out of sight in the boot of your car.

Computers

Where computers are networked, access to personal and special categories of personal information is restricted by password to authorised personnel only.

Computer monitors in the reception area, or other public areas, should be positioned in such a way so that passers-by cannot see what is being displayed. If this is not possible then privacy screens should be used on the monitor to afford this level of protection. If working in a public area, eg receptions, you should lock your computer when leaving it unattended.

Firewalls and virus protection to be employed at all times to reduce the possibility of hackers accessing our system and thereby obtaining access to confidential records.

Documents should only be stored on the server or cloud-based systems and not on individual computers.

Where computers or other mobile devices are taken for use off the premises the device must be password protected.

Cloud Computing

When commissioning cloud based systems, IADA Limited will satisfy themselves as to the compliance of data protection principles and robustness of the cloud based providers.

Direct Marketing

Direct Marketing is a communication that seeks to increase customer base and revenue. The communication may be in any of a variety of formats including mail, telemarketing and email. The responses should be recorded to inform the next communication. IADA Limited will not share or sell its database(s) with outside organisations.

IADA Limited holds information on our staff, customers and suppliers to whom we will from time to time send copies of any newsletters, magazine and details of other publications that may be of interest to them. Specific consent to contact will be sought from our staff, customers and any suppliers, including which formats they prefer (eg mail, email, phone etc) before making any communications.

We recognise that suppliers, staff, and customers for whom we hold records have the right to unsubscribe from our mailing lists. This wish will be recorded on their records and will be excluded from future contacts.

The following statement is to be included on any forms used to obtain personal data:

> We promise never to share or sell your information to other organisations or businesses and you can opt out of our communications at any time by telephoning 0114 2436143 or by writing to IADA Limited, 23-25 Stevenson Street, Sheffield, S9 3XG or by sending an email to admin@iadaltd.co.uk

Privacy Statements

Any documentation which gathers personal and/or special categories of personal data should contain the following Privacy Statement information:

- Explain who we are
- What we will do with their data
- Who we will share it with
- Consent for marketing notice
- How long we will keep it for
- That their data will be treated securely
- How to opt out
- Where they can find a copy of the full notice

A fuller Privacy Statement will also be published on our website.

Personnel Records

The Regulations apply equally to customer and staff records. IADA Limited may at times record special categories of personal data with the customer's consent or as part of a staff member's contract of employment.

Confidentiality

When working from home, or from some other off-site location, all data protection and confidentiality principles still apply. All computer data, e.g. documents and programmes related to work for IADA Limited should not be stored on any external hard disk or on a personal computer. If documents need to be worked on at a non-networked computer they should be saved onto a USB drive which should be password protected.

Workstations in areas accessible to the public, e.g. reception or trading office, should operate a clear desk practice so that any paperwork, including paper diaries, containing personal and/or special categories of personal data is not left out on the desk where passers-by could see it.

When sending emails to outside organisations, e.g. suppliers, care should be taken to ensure that any identifying data is removed (e.g. initials or email addresses, etc.). Confidential and/or special categories of personal information should be written in a separate document which should be password protected before sending. Wherever possible, this document should be 'watermarked' confidential.

Any paperwork kept away from the office (eg personal data kept at home by a worker) should be treated as confidential and kept securely as if it were held in the office. Documents should not be kept in open view (eg on a desktop) but kept in a file in a drawer or filing cabinet as examples, the optimum being a locked cabinet but safely out of sight is a minimum requirement.

Retention of Records

Paper records should be retained for the following periods at the end of which they should be shredded:

- Supplier records – 6 years after ceasing to be a supplier.
- Staff records – 6 years after ceasing to be a member of staff.
- Unsuccessful staff application forms – 6 months after vacancy closing date.
- Volunteer records – 6 years after ceasing to be a volunteer.
- Timesheets and other financial documents – 7 years.
- Employer's liability insurance – 40 years.
- Other documentation should be destroyed as soon as it is no longer needed for the task in hand.

Archived records should clearly display the destruction date.

What to Do If There Is a Breach

If you discover, or suspect, a data protection breach you should report this to your line manager who will review the systems, in conjunction with the Data Compliance Officer, to prevent a reoccurrence. The Non-Executive Chairman should be informed of the breach, action taken and outcomes to determine whether it needs to be reported to the Information Commissioner and also for reporting to the IADA Members. There is a time limit for reporting breaches to ICO so the Non-Executive Chairman should be informed without delay.

Any deliberate or reckless breach of this Data Protection Policy by an employee may result in disciplinary action which may result in dismissal.

The Rights of an Individual

Under the Regulations an individual has the following rights with regard to those who are processing his/her data:

- Personal and special categories of personal data cannot be held without the individual's consent.

- Data cannot be used for the purposes of direct marketing of any goods or services if the Data Subject has declined their consent to do so.

- Individuals have a right to have their data erased and to prevent processing in specific circumstances:
    - Where data is no longer necessary in relation to the purpose for which it was originally collected
    - When an individual withdraws consent
    - When an individual objects to the processing and there is no overriding legitimate interest for continuing the processing
    - Personal data was unlawfully processed
- An individual has a right to restrict processing – where processing is restricted, IADA Limited is permitted to store the personal data but not further process it. IADA Limited can retain just enough information about the individual to ensure that the restriction is respected in the future.
- An individual has a 'right to be forgotten'.

IADA Limited will not undertake direct telephone marketing activities under any circumstances.

Data Subjects can ask, in writing to the Non-Executive Chairman, to see all personal data held on them, including e-mails and computer or paper files. The Data Processor (IADA Limited) must comply with such requests within 30 days of receipt of the written request.

Powers of the Information Commissioner

The following are criminal offences, which could give rise to a fine and/or prison sentence

- The unlawful obtaining of personal data.
- The unlawful selling of personal data.
- The unlawful disclosure of personal data to unauthorised persons.

Further Information

Further information is available at www.informationcommissioner.gov.uk

Details of the Information Commissioner

The Information Commissioner's office is at:

Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF

Switchboard*:* 01625 545 700
Email: mail@ico.gsi.gov.uk
Data Protection Help Line: 01625 545 745
Notification Line: 01625 545 740

Revision History

Revision date	Summary of Changes	Other Comments
8th April 2020	Routine review of any updates to GDPR Policy	

23-25 Stevenson Road, Sheffield S9 3XG

GDPR - INFORMATION SECURITY POLICY

1. INTRODUCTION

We provide employees with access to various computing, telephone and postage facilities ("the Facilities") to allow them to undertake the responsibilities of their position and to improve internal and external communication.

2. SCOPE AND APPLICABILITY

This Policy applies to all individuals that use or operate within our IT Systems, including networks, Laptops, desktops, telephones or any other facility that is provided for communication purposes.

This Policy applies to the use of:

- local, inter-office, national and international, private or public networks (including the Internet and Intranet) and all systems and services accessed through those networks;
- desktop, portable and mobile computers and applications (including personal digital assistants (PDAs);
- mobile telephones
- Electronic mail (Email) and messaging services.

Observation of this Policy is mandatory and forms part of the Terms and Conditions of Employment. Misuse of the Facilities will be treated as gross misconduct and may lead to dismissal.

3. PURPOSE

This Policy sets out the Company's policy on the use of the Facilities and it includes:

- Responsibilities and potential liability when using the Facilities;
- The monitoring policies adopted by the Company; and
- Guidance on how to use the Facilities.

This Policy has been created to:

- Ensure compliance with all applicable laws relating to data protection, information security and compliance monitoring;
- Protect the Company and its employees from the risk of financial loss, loss of reputation or libel; and
- Ensure that the Facilities are not used to cause harm or damage to any person or organisation.

4. COMPUTER FACILITIES - USE OF COMPUTER SYSTEMS

To comply with this policy it should be noted that unless written prior authorisation has been received by departmental managers, the Facilities must be used for business purposes only.

To maintain the confidentiality of information held on or transferred via the Company's Facilities, security measures are in place and must be followed always. A log-on ID and password is required for access to the Company's network. Despite the use of a password, the Company reserves the right to override passwords and obtain access to any part of the Facilities.

Individuals are ultimately responsible for keeping passwords secure. They must not give it to anyone, including colleagues, except as expressly authorised by the Company. Passwords should be changed if requested by Management or by the IT company and any changes must be advised to Management.

Individuals are expressly prohibited from using the Facilities for the sending, receiving, printing or otherwise disseminating information which is the confidential information of the Company or its clients other than in the normal and proper course of carrying out duties for the Company.

5. IT SECURITY PROCEDURES

To ensure proper use of computers, all individuals must adhere to the following practices:

- Anti-virus software must be kept running always;
- All users accessing domain joined computer must seek IT permission to be able to use USB storage on the company network. If this permission is not requested, USB/CD media will be rendered un-accessible.
- Obvious passwords such as birthdays and spouse names etc. must be avoided. The most secure passwords are random combinations of letters and numbers. Password minimum complexity requirements are in force when creating/updating existing passwords;
- When you are sending data or software to an external party by Data storage media always ensure that the disk has been checked for viruses by the Group IT Support Department and password protected if required, before sending it;
- All files must be stored on the network drive which is backed up regularly to avoid loss of information; and
- Always log off the network before leaving your computer for long periods of time or overnight.

6. SOFTWARE

Software piracy could expose both the Company and the user to allegations of intellectual property infringement. The Company are committed to following the terms of all software licences to which the Company is a contracting party. This means that:

- Software must not be installed onto any of the Company's computers unless this has been approved in advance by the Group IT Support Department. They will be responsible for establishing that the

appropriate licence has been obtained, that the software is virus free and compatible with the computer Facilities; and

- Software should not be removed from any computer nor should it be copied or loaded on to any computer without the prior consent of the IT Department.

7. LAPTOP COMPUTERS

At various times during employment with the Company, individuals may use a laptop. These computers, along with related equipment and software are subject to all the Company's policies and guidelines governing non-portable computers and software (see two paragraphs in software section above). However, use of a laptop creates additional problems especially in respect of potential breaches of confidentiality. When using a laptop:

- Individuals are responsible for all equipment and software until it is returned. The laptop must be kept secure always;
- It should only be used by the person authorised to use the equipment and software;
- Individuals must not load or install files from any sources without the Group IT Support Department inspecting such files for viruses;
- All data kept on the laptop must be backed up regularly to protect data against theft or mechanical failure or corruption;
- Individuals should password protect confidential data on disks or on the hard drive to protect against theft;
- If individuals become aware of any mechanical, electronic, or software defects or malfunctions, they should immediately bring such defects or malfunctions to the attention of the Group IT Support Department;
- Upon the request of the Company at any time, for any reason, Individuals will immediately return any laptop, equipment and all software to the Company; and
- If for any reasons individuals are using their own laptop to connect with the Company's network or to transfer data between the laptop and any of the Company's computers it is essential that they ensure that they you have obtained prior consent from the Group IT Support Department, and their Department Head to comply with its instructions and ensure that any data downloaded or uploaded is free from viruses.

8. E-MAIL (INTERNAL OR EXTERNAL USE)

Internet e-mail is not a secure medium of communication – it can be intercepted and read. Do not use it to say anything that the Company or individuals would not wish to be made public. If individuals are sending confidential information by e-mail this should be sent using password protected attachments.

E-mail should be treated as any other documentation. If an individual would normally retain a certain document in hard copy you should retain the e-mail.

Do not forward e-mail messages unless the original sender is aware that the message may be forwarded. If you would not have forwarded a copy of a paper memo with the same information do not forward the e-mail.

E-mail inboxes should be checked on a regular basis.

As with many other records, e-mail may be subject to discovery in litigation. Like all communications, individuals should not say anything that might appear inappropriate or that might be misinterpreted by a reader or bring the Company into disrepute.

Individuals should not use the Company email system for private messages during work activities unless necessary and in these circumstances the following message should be contained within the email that is sent:

"This e-mail does not reflect the views or opinions of our organisation"

Use of e-mail facilities for personal use is permitted providing that:

- Such e-mails do not contain information or data that could be obscene, racist, sexist, otherwise offensive and provided that such use is not part of a pyramid or chain letter; and
- Such e-mails are not used for trading or carrying out any business activity other than Company business.

If individuals are away from the office and use e-mail as an external means of communication they must ensure that the autoreply service is used to inform the sender that they are unavailable. Failure to do so could lead to disciplinary action. If there is any doubt as to how to use these Facilities please contact the Group IT Support Department.

Viewing, displaying, storing (including data held in RAM or cache) or disseminating materials (including text and images) that could be obscene, racist, sexist, or otherwise offensive may constitute harassment and such use of the Facilities is strictly prohibited.

NB: The legal focus in a harassment case is the impact of the allegedly harassing material on the person viewing it, not how the material is viewed by the person sending or displaying it.

9. INTERNET

Use of the Internet, or Internet services, by unauthorised users is strictly prohibited. Individuals are responsible for ensuring that they are the only person using the authorised Internet account and services.

Downloading any files from the Internet using the computer Facilities is not permitted. If there is a file or document on the Internet that is required, the individual should contact the Group IT Support Department to decide for it to be evaluated and checked for viruses. It will be at the discretion of the Group IT Support Department on whether to allow such download.

Viewing, downloading, storing (including data held in RAM or cache) displaying or disseminating materials (including text and images) that could be obscene, racist, sexist, or otherwise offensive may constitute harassment and such use is strictly prohibited.

NB: The legal focus in a harassment case is the impact of the allegedly harassing material on the person viewing it, not how the material is viewed by the person sending or displaying it.

Posting information on the Internet, whether on a newsgroup, via a chat room or via e-mail is no different from publishing information in the newspaper. If a posting is alleged to be defamatory, libellous, or harassing, the employee making the posting and the Company could face legal claims for monetary damages.

Using the Internet for trading or carrying out any business activity other than Company business is strictly prohibited.

For the avoidance of doubt the matters set out above include use of 3G/4G Data.

10. MONITORING POLICY

The Policy of the Company is that we monitor use of the Facilities.

The Company recognises the importance of an individual's privacy but needs to balance this against the requirement to protect others and preserve the integrity and functionality of the Facilities.

The Company may from time to time monitor the Facilities. Principle reasons for this are to:

- Detect any harassment or inappropriate behaviour by employees, ensuring compliance with contracts of employment and relevant policies including the health and safety, ethical and sex discrimination policies;

- Ensure compliance of this Policy;
- Detect and enforce the integrity of the Facilities and any sensitive or confidential information belonging to or under the control of the Company;
- Ensure compliance by users of the Facilities with all applicable laws (including Data Protection), regulations and guidelines published and in force from time to time; and
- Monitor and protect the well-being of employees.

The Company may adopt at any time many methods to monitor use of the Facilities. These may include:

- Recording and logging of internal, inter-office and external telephone calls made or received by employees using its telephone network (including where possible mobile telephones). Such recording may include details of length, date and content;

- Recording and logging the activities by individual users of the Facilities. This may include opening e-mails and their attachments, monitoring Internet usage including time spent on the Internet and web sites visited;
- Physical inspections of individual user's computers, software and telephone messaging services;
- Periodic monitoring of the Facilities through third party software including real time inspections;
- Physical inspection of an individual's post; and
- Archiving of any information obtained from the above including e-mails, telephone call logs and Internet downloads.

If at any time an employee wishes to use the Facilities for private purposes without the possibility of such use being monitored they should contact their Department Head or the nominated deputy. This person will consider such request and any restrictions upon which such consent is to be given. If such request is granted the Company (unless required by law) will not monitor the applicable private use.

11. BUILDING SECURITY

Confidential and sensitive data is secured in the building. This is both in paper form (such as files of paperwork) and electronically (such as computers, storage devices and servers).

To improve the security and confidentiality of information, we require the following:

1. Do not allow entry to our premises to any unknown person
2. Ensure all visitors are signed in and are issued with an appropriate visitor pass and that they are advised to wear these passes visibly always
3. If you see someone you do not recognise and you cannot see that they are wearing a pass, ask to see their pass
4. If you see someone you do not recognise and they cannot show you a pass, immediately escort the person to reception to be signed in
5. Do not allow visitors to access roam the premises without being accompanied
6. Ensure you collect your visitors from reception
7. Ensure passes are returned and the visitor is signed out
8. Do not hold door open for people you do not recognise
9. Clock in and clock out in the instructed manner
10. Report anything suspicious to your manager

12. CLEAR DESK

To improve the security and confidentiality of information, we have adopted a Clean Desk Policy for computer and printer workstations.

This ensures that all sensitive and confidential information, whether it be on paper, a storage device, or a hardware device, is properly locked away or disposed of when a workstation is not in use. This policy will

reduce the risk of unauthorised access, loss of, and damage to information during and outside of normal business hours or when workstations are left unattended.

Whenever a desk is unoccupied for an extended period the following will apply:

1. All sensitive and confidential paperwork must be removed from the desk and locked in a drawer or filing cabinet. This includes mass storage devices such as CDs, DVDs, and USB drives.
2. All waste paper which contains sensitive or confidential information must be placed in the designated confidential waste bins. Under no circumstances should this information be placed in regular waste paper bins.
3. Computer workstations must be locked when the desk is unoccupied and completely shut down at the end of the work day.
4. Laptops, tablets, and other hardware devices must be removed from the desk and locked in a drawer or filing cabinet.
5. Keys for accessing drawers or filing cabinets should not be left unattended at a desk.
6. Printers and fax machines should be treated with the same care under this policy:
    a. Any print jobs containing sensitive and confidential paperwork should be retrieved immediately. When possible, the “Locked Print” functionality should be used.
    b. All paperwork left over at the end of the work day will be properly disposed of.

13. GENERAL GUIDANCE

Never leave any equipment or data (including client files, laptops, computer equipment, mobile phones and PDAs) unattended on public transport or in an unattended vehicle.

Observation of this Policy is mandatory and forms part of the Terms and Conditions of Employment. Misuse of the Facilities or a breach of this policy may be treated as gross misconduct and may lead to dismissal.

I hereby confirm that I have received a copy of the GDPR Information Security Policy and accept that it forms part of my Contract of Employment

…….
Employee’s Name

……
Employee’s Signature

……
Date

(To be returned to the Company and kept on the employee’s personnel file)