

**Employee**

**Handbook**

Contents Page

Introduction

Data Protection & Access to Personal Records

References

Changes in Personal Details

Equal Opportunities

Policy to Prevent Harassment & Bullying

Maternity Paternity & Adoption

Attendance, Timekeeping & Absence

Flexible Working

Parental Leave

Annual Leave

Time Off in Lieu

Time Off for Emergency Leave for Dependents

Bereavement

Disciplinary Procedure

Grievance Procedure

Pensions

Retirement

Expenses

Season Ticket Loan

Smoking

Dress Code

Gifts & Bribery

Email, Internet, Information Technology, Software & Mobile Telephony

Monitoring at Work

Health & Safety

Eye Care Policy

Lone working and Personal Security

Right of Search

Charity Property

Protected Disclosures

Anti-Slavery Policy

Confirmation of Receipt of Handbook

## Introduction

#### **On behalf of Kingston Healthwatch we want to welcome you.**

This handbook has been written to provide a guide to employees regarding the Charity’s policies and procedures. It is designed to be accessible and easy to understand and should be a useful guide for all employees

You will be informed of any other specific rules with which you must comply by your department manager, who will also be able to assist with any queries that you may have regarding your employment.

The policies and procedures set out in this handbook apply to all employees. They do not form part of your contract of employment with us. This handbook may be reviewed and updated from time to time to ensure that the Charity meets it statutory legal obligations.

We hope that you become a key member of the charity and that you will have a long, happy and successful career with us.

## Data Protection & Access to Personal Records

EMPLOYEE GENERAL DATA PROTECTION POLICY

1. Introduction

This Policy sets out the Employer’s and Employees’ obligations in respect of Employees’ personal data under the General Data Protection Regulation (“GDPR”), which comes into force on the 25th May 2018.

1. The Data Protection Principles

This Policy aims to ensure the Employer’s and the Employees’ compliance with the GDPR. The GDPR sets out the following principles, which any party handling personal data must comply. All personal data must be:

* + 1. processed lawfully, fairly, and in a transparent manner in relation to the Employee;
		2. collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest or as is required by law shall not be considered to be incompatible with the initial purposes;
		3. adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed;
		4. accurate and where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate is erased, or rectified without undue delay;
		5. kept in a form, which permits identification of Employees for no longer than is necessary for the purposes for which the personal data is processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, or as is required by law, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights of the Employee;
		6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures;
1. Lawful, Fair, and Transparent Data Processing
	* 1. The GDPR seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the Employee (“data subject”). The GDPR states that processing of personal data shall be lawful if at least one of the following applies:
			+ 1. The data subject has given consent to the processing of their personal data for one or more specific purposes;
				2. The 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 with them;
				3. The processing is necessary for compliance with a legal obligation to which the data controller is subject;
				4. The processing is necessary to protect the vital interests of the data subject or of another natural person;
				5. The 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 data controller; or
				6. The processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.
		2. If the personal data in question is “special category data” (also known as “sensitive personal data” (for example, data concerning the data subject’s race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life, or sexual orientation), at least one of the following conditions must be met:
			+ 1. The data subject has given their explicit consent to the processing of such data for one or more specified purposes;
				2. The processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment, social security, and social protection law;
				3. The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
				4. The data controller is a foundation, association, or other non-profit body with a political, philosophical, religious, or trade union aim, and the processing is carried out in the course of its legitimate activities, provided that the processing relates solely to the members or former members of that body or to persons who have regular contact with it in connection with its purposes and that the personal data is not disclosed outside the body without the consent of the data subjects;
				5. The processing relates to personal data which is clearly made public by the data subject;
				6. The processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity;
				7. The processing is necessary for substantial public interest reasons, which shall be proportionate to the aim pursued, shall respect the essence of the right to data protection, and shall provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject;
				8. The processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee, for medical diagnosis, for the provision of health or social care or treatment, or the management of health or social care systems.
				9. The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes or as is required by law.
2. Explicit, and Legitimate Purposes
	* 1. The Employer collects and processes the personal data of Employees, this includes:
			+ 1. Personal data collected directly from employee data subjects**,** and
				2. Personal data obtained from third parties.
		2. The Employer will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which employee data subjects have been informed or will be informed.
3. Accuracy of Data and Keeping Data Up-to-Date
	* 1. The Employer shall ensure that all personal data collected, processed, and held by it is kept accurate and up-to-date. This includes, but is not limited to, the rectification of personal data at the request of an employee data subject.
		2. The accuracy of personal data shall be checked when it is collected and at regular intervals thereafter. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.
4. Data Retention
	* 1. The Employer shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed.
		2. When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.
5. Secure Processing

The Employer shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage.

1. Accountability and Record-Keeping
	* 1. The Employer shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy.
		2. The Employer shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:
			+ 1. The name and details of the Employer and any applicable third-party data processors;
				2. The purposes for which the Employer collects, holds, and processes personal data;
				3. Details of the categories of personal data collected, held, and processed by the Employer, and the categories of employee data subject to which that personal data relates;
				4. Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards;
				5. Details of how long personal data will be retained by the Employer; and
				6. Details of all technical and organisational measures taken by the Employer to ensure the security of personal data.
2. Data Protection Impact Assessments
	* 1. The Employer shall carry out Data Protection Impact Assessments for uses of personal data and shall address the following:
			+ 1. The type(s) of personal data that will be collected, held, and processed;
				2. The purpose(s) for which personal data is to be used;
				3. The Employer’s objectives;
				4. How personal data is to be used;
				5. The parties (internal and/or external) who are to be consulted;
				6. The necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;
				7. Risks posed to employee data subjects;
				8. Risks posed both within and to the Employer; and
				9. Proposed measures to minimise and handle identified risks.
3. Data Subject Access
	* 1. Employee data subjects may make subject access requests (“SARs”) at any time to find out more about the personal data which the Employer holds about them, what it is doing with that personal data, and why.
		2. Employees wishing to make a SAR should do using a Subject Access Request Form, sending the form to the Employer’s Data Protection Officer.
		3. Responses to SARs shall normally be made within one month of receipt, however this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the employee data subject shall be informed.
		4. All SARs received shall be handled by the Employer’s Data Protection Officer.
		5. The Employer does not charge a fee for the handling of normal SARs. The Employer reserves the right to charge reasonable fees for additional copies of information that has already been supplied to an employee data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.
4. Rectification of Personal Data
	* 1. Employee data subjects have the right to require the Employer to rectify any of their personal data that is inaccurate or incomplete.
		2. The Employer shall rectify the personal data in question, and inform the employee data subject of that rectification, within one month of the employee data subject informing the Employer of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the employee data subject shall be informed.
		3. In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.
5. Erasure & Ceasing Processing of Personal Data
	* 1. Employee data subjects have the right to request that the Employer erases the personal data it holds about them in certain circumstances, but it should be understood that usually personal data is processed by the Employer for an overriding legitimate interest with regard to an Employee’s employment. Therefore in many circumstances personal data cannot be erased or processing cannot be ceased.
		2. If it is agreed with the Employee to erase or cease processing personal data for a legitimate reason the Employer shall cease such processing immediately, unless it can be demonstrated that the Employer’s legitimate grounds for such processing override the employee data subject’s interests, rights, and freedoms, or that the processing is necessary for the conduct of legal or potential legal claims.
6. Personal Data

The Employer holds personal data that is directly relevant to its employees. That personal data shall be collected, held, and processed in accordance with employee data subjects’ rights and the Employer’s obligations under the GDPR and with this Policy.

Identification information relating to employees:

* + - * 1. Name;
				2. Contact Details;
				3. <<add further data as required>>.
		1. Equal opportunities monitoring information **[**(such information shall be anonymised where possible)**]**:
			- 1. Age;
				2. Gender;
				3. Ethnicity;
				4. Nationality;
				5. Religion;
				6. <<add further data as required>>.
		2. Health records:
			- 1. Details of sick leave;
				2. Medical conditions;
				3. Disabilities;
				4. Prescribed medication;
				5. <<add further data as required>>.
		3. Employment records:
			- 1. Interview notes;
				2. CVs, application forms, covering letters, and similar documents;
				3. Assessments, performance reviews, and similar documents;
				4. Details of remuneration including salaries, pay increases, bonuses, commission, overtime, benefits, and expenses;
				5. Details of trade union membership (where applicable);
				6. Employee monitoring information;
				7. Records of disciplinary matters including reports and warnings, both formal and informal;
				8. Details of grievances including documentary evidence, notes from interviews, procedures followed, and outcomes;
				9. <<add further data as required>>.
1. Health Records
	* 1. The Employer holds health records Employee data subjects, which are used to assess the health, wellbeing, and welfare of employees and to highlight any issues, which may require further investigation. In particular, the Employer places a high priority on maintaining health and safety in the workplace, on promoting equal opportunities, and on preventing discrimination on the grounds of disability or other medical conditions. In most cases, health data on employees falls within the GDPR’s definition of special category data. Any and all data relating to employee data subjects’ health, therefore, will be collected, held, and processed strictly in accordance with the conditions for processing special category personal data, as set out in this Policy.
		2. Health records will only be collected, held, and processed to the extent required to ensure that employees are able to perform their work correctly, legally, safely, and without unlawful or unfair impediments or discrimination.
2. Benefits
	* 1. In cases where employee data subjects are enrolled in benefit schemes which are provided by the Employer, it may be necessary from time to time for third party organisations to collect personal data from relevant employee data subjects.
		2. Prior to the collection of such data, employee data subjects will be fully informed of the personal data that is to be collected, the reasons for its collection, and the way(s) in which it will be processed.
		3. The Employer shall not use any such personal data except insofar as is necessary in the administration of the relevant benefits schemes.
3. Employee Monitoring
	* 1. The Employer may from time to time monitor the activities of employee data subjects. Such monitoring may include, but will not necessarily be limited to, Internet and email monitoring. In the event that monitoring of any kind is to take place (unless exceptional circumstances, such as the investigation of criminal activity or a serious disciplinary matter, justify covert monitoring), employee data subjects will be informed of the exact nature of the monitoring in advance.
		2. Monitoring should not (unless exceptional circumstances justify it, as above) interfere with an employee’s normal duties.
		3. Monitoring will only take place if the Employer considers that it is necessary to achieve the benefit it is intended to achieve. Personal data collected during any such monitoring will only be collected, held, and processed for reasons directly related to (and necessary for) achieving the intended result and, at all times, in accordance with employee data subjects’ rights and the Employer’s obligations under the GDPR.
		4. The Employer shall ensure that there is no unnecessary intrusion upon employee data subjects’ personal communications or activities, unless the employee data subject in question is using Employer equipment or other facilities including, but not limited to, Employer email, the Employer intranet, or a virtual private network (“VPN”) service provided by the Employer for employee use.
4. Data Security - Transferring Personal Data and Communications

The Employer shall ensure that the following measures are taken with respect to all communications and other transfers involving personal data (including, but not limited to, personal data relating to employees):

* + 1. All emails containing personal data must be encrypted;
		2. All emails containing personal data must be marked “confidential”;
		3. Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;
		4. Where personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data;
		5. Where personal data is to be transferred in hardcopy form it should be passed directly to the recipient; and
		6. All personal data to be transferred physically, whether in hardcopy form or on removable electronic media shall be transferred in a suitable container marked “confidential”.
1. Data Security - Storage

The Employer shall ensure that the following measures are taken with respect to the storage of personal data (including, but not limited to, personal data relating to employees):

* + 1. All electronic copies of personal data should be stored securely using passwords and data encryption;
		2. All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar;
		3. All personal data stored electronically should be backed up with backups stored. All backups should be encrypted.
		4. No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets, and smartphones), whether such device belongs to the Employer or otherwise without the formal written approval of a Officer and in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is necessary; and
		5. No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Employer where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the GDPR (which may include demonstrating to the Employer that all suitable technical and organisational measures have been taken).
1. Data Security - Disposal

When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of.

1. Data Security - Use of Personal Data

The Employer shall ensure that the following measures are taken with respect to the use of personal data:

* + 1. No personal data may be shared informally and if an employee, agent, sub-contractor, or other party working on behalf of the Employer requires access to any personal data that they do not already have access to, such access should be formally requested from a Senior Manager of the Employer.
		2. No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Employer or not, without the authorisation of a Senior Manager of the Employer.
		3. Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors, or other parties at any time;
		4. If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it; and
1. Data Security - IT Security

The Employer shall ensure that the following measures are taken with respect to IT and information security:

* + 1. All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised.
		2. Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of the Employer, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method.
		3. No software may be installed on any Employer-owned computer or device without the prior approval of a Senior Manager of the Employer.
1. Organisational Measures

The Employer shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

* + 1. All employees, agents, contractors, or other parties working on behalf of the Employer shall be made fully aware of both their individual responsibilities and the Employer’s responsibilities under the GDPR.
		2. Only employees, agents, sub-contractors, or other parties working on behalf of the Employer that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Employer;
		3. All employees, agents, contractors, or other parties working on behalf of the Employer handling personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise;
		4. All personal data held by the Employer shall be reviewed periodically.
		5. All employees, agents, contractors, or other parties working on behalf of the Employer handling personal data will be bound to do so in accordance with the principles of the GDPR and this Policy;
		6. All agents, contractors, or other parties working on behalf of the Employer handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Employer arising out of this Policy and the GDPR.
1. Transferring Personal Data to a Country Outside the EEA
	* 1. The Employer may from time to time transfer (‘transfer’ includes making available remotely) personal data to countries outside of the EEA.
		2. The transfer of personal data to a country outside of the EEA shall take place only if one or more of the following applies:
			+ 1. The transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the European Commission has determined ensures an adequate level of protection for personal data;
				2. The transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the European Commission; compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner’s Office); certification under an approved certification mechanism (as provided for in the GDPR); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority;
				3. The transfer is made with the informed consent of the relevant employee data subject(s);
				4. The transfer is necessary for the performance of a contract between the employee data subject and the Employer (or for pre-contractual steps taken at the request of the employee data subject);
				5. The transfer is necessary for important public interest reasons;
				6. The transfer is necessary for the conduct of legal claims;
				7. The transfer is necessary to protect the vital interests of the employee data subject or other individuals where the employee data subject is physically or legally unable to give their consent; or
				8. The transfer is made from a register that, under UK or EU law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.
2. Data Breach Notification
	* 1. All personal data breaches must be reported immediately to NAME.
		2. If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of Employee data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Officer must ensure that the Information Commissioner’s Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.
		3. In the event that a personal data breach is likely to result in a high risk to the rights and freedoms of employee data subjects, the Data Protection Officer must ensure that all affected employee data subjects are informed of the breach directly and without undue delay.
		4. Data breach notifications shall include the following information:
			+ 1. The categories and approximate number of employee data subjects concerned;
				2. The categories and approximate number of personal data records concerned;
				3. The name and contact details of the Employer’s data protection officer (or other contact point where more information can be obtained);
				4. The likely consequences of the breach;
				5. Details of the measures taken, or proposed to be taken, by the Employer to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

## References

Any reference requests made by former employees must be referred to an Officer of the Charity who will respond on behalf of the Charity.

No employees have authority to complete a reference on behalf of the Charity for any current or former employee.

Charity policy is to provide factual references only.

## Changes in Personal Details

It is your responsibility to keep the Charity informed of any changes in your personal details. Please inform a Officer of the Charity of any changes such as a change of address, marital status, change of telephone number etc.

If you are convicted of a criminal offence, including driving offences, whilst in your employment you must notify an Officer of the Charity immediately.

## Equal Opportunities

The Charity is committed to giving equal opportunities to all employees and prospective employees irrespective of their gender, gender re-assignment, sexual orientation, marital status, race, ethnic origin, colour, nationality, disability, religion or belief, trade union membership or age.

In giving equal opportunities we actively encourage all of our employees to achieve their full potential and take all reasonable steps to ensure that employees are employed and promoted within the Charity on the basis of their abilities and qualifications:

* The Charity uses fair and objective criteria when recruiting and selection procedures will be reviewed from time to time to ensure that they are not discriminatory.
* Job specifications will be limited to those requirements necessary for the effective performance of the job.
* All managers will be trained in equal opportunities.
* Every effort will be made by the Charity to ensure that all employees are treated equally.

In return all employees have a responsibility to ensure that they work in accordance with the Charity’s equal opportunity policy. If you consider at any time that the Charity is not practising equal opportunities for any reason, then you can discuss it with your Manager. If you are not satisfied with the outcome then you are encouraged to use the Charity’s grievance procedure.

## Policy to Prevent Harassment & Bullying

The Charity will take all reasonable steps to ensure the workplace is free from harassment and bullying. It is recognised that both are serious offences and those accused of causing them or participating in them will be dealt with via our disciplinary procedure and in certain circumstances could be dismissed.

Harassment occurs where a person engages in unwanted conduct which has the purpose or effect of violating the other’s dignity at work or creating an intimidating, hostile, degrading, humiliating or offensive work environment for the other person.

Bullying can take the form of verbal or non-verbal conduct which could be regarded as intimidating behaviour.

Examples of harassment and bullying include, but are not limited to:

* sexual or racial comments or banter; physical contact of a sexual or bullying nature
* the display of sexual or racial material (even if not directed at the complainant)
* personal remarks about colleagues especially those reporting to you
* over-demanding work requirements

It is for the complainant to decide for themselves what they regard as bullying or harassment.

Bullying or harassment will not be tolerated away from your normal place of work such as at training courses or social events.

The Charity also recognises that advances in mobile phone technology and the increased use of social networking sites means that bullying and harassment can take place outside of the workplace. This is often referred to as “cyber bullying”.

Any employees who conduct bullying, harassment or victimisation using such tools will be dealt with via the disciplinary procedure and in certain circumstances could be dismissed.

Bullying, harassment or victimisation in such circumstances could include, but is not limited to:

* posting offensive or threatening comments or photographs about colleagues using blogs or social networking sites
* deliberately excluding colleagues from “friendship circles”

If you believe that you are being bullied or harassed then in the first instance you can discuss your concerns with your Manager informally. If the complaint is about your Manager or you feel you cannot discuss it with your Manager then please inform another member of the management team. If you believe that you are being harassed by people who are not employees of the Charity, such as customers or clients then discuss your concerns with your Manager. If you feel that you cannot discuss it with your Manager then please inform another member of the management team.

Any claims of bullying or harassment will be taken seriously and a thorough and fair investigation will take place. You will normally be informed of the outcome within 14 days receipt of the original complaint.

If after you have raised your concerns either formally or informally you are not satisfied with the outcome then you are able to utilise the Charity’s grievance procedure. Any legitimate complaint or concern at any stage will be treated with discretion and confidentiality and will not have any detrimental effect to your employment with the Charity.

## Maternity, Paternity & Adoption

Working parents have rights relating to maternity, paternity & adoption leave.

The Charity will at all times comply with current legislation in force at that time regarding entitlement to payment and leave.

The current legislation regarding maternity leave, pay and rights can be found here -

<https://www.gov.uk/maternity-pay-leave>

The current legislation regarding paternity leave, pay and rights can be found here -

<https://www.gov.uk/paternity-pay-leave>

The current legislation regarding adoption leave, pay and rights can be found here -

<https://www.gov.uk/employers-adoption-pay-leave>

Please contact your Manager if you require any information about your entitlements.

Telling us you are pregnant:

* You can tell us that you are pregnant as soon as you want to. This can be before you have decided when to take maternity leave. You will need to tell your Manager if you want to take paid time off for ante-natal appointments.
* You are protected from dismissal and unfair treatment on the grounds of pregnancy and from any health or safety risks to you or your baby as soon as we know that you are pregnant.

Ante-natal care

All pregnant employees are entitled to paid time off work for ante-natal care which your doctor, midwife or health visitor advises. Except in the case of your first appointment, you must be prepared to show us on request:

* a certificate from your doctor, midwife or health visitor confirming you are pregnant
* an appointment card or some other document that confirms the appointment

Maternity, Paternity & Adoption Leave & Pay and Shared Parental Leave

Please contact your Manager to establish your entitlement to statutory maternity, paternity and adoption leave and pay and Shared Parental Leave.

## Attendance, Timekeeping & Absence

You are expected to be punctual at all times and not to leave your place of work without permission from your Manager.

If you are late for work your Manager will have a discussion with you to ascertain why you were late and to agree with you any actions to prevent this from occurring in future.

If you need to visit your doctor or dentist or similar, appointments should be made outside of working hours whenever possible. If you are unable to do this, please inform your Manager as soon as possible for their approval. You may be required to make up your time away from work.

All employees are encouraged to maintain a high level of attendance.

The Charity recognises that some levels of absence may be necessary due to sickness or other situations and the Charity will be supportive in genuine circumstances.

Unauthorised or excessive absences and lateness will not be acceptable without reasonable justification and may result in disciplinary action being taken following investigation.

In the event of illness please notify your Manager on the first day of illness as soon as you are able and no later than 10:00 a.m., by telephone, stating the reason for your absence and the likely duration. You should make every effort to report any absence yourself, however in extreme circumstances for instance if you are hospitalised then it is permissible for someone else to inform your manager using the above procedure. Texting or emailing the Charity of your absence or illness is not acceptable and may result in disciplinary action.

If your Manager is unavailable, please speak to another Manager or a Officer of the Charity.

Failure to do so may render you subject to disciplinary action and may also prevent you from receiving sick pay.

If your absence continues you will be required to contact your manager on the 4th and 8th day of absence to update them regarding your situation.

You will be required to complete an absence declaration form on your return to work in respect of absences lasting up to 7 calendar days.

On the 8th calendar day of any absence you must provide a medical certificate from your General Practitioner stating the reason for the absence and provide further medical certificates covering any ongoing period of absence.

We reserve the right to ask you to produce a medical certificate for any periods of absence including the first 3 days and to undergo a medical examination at any time during your employment.

Every employee on returning to work following a period of absence will have a return to work interview. On your return to work you must make your manager aware of any restrictions that have been placed on you with regard to carrying out your normal duties. A risk assessment may be carried out if appropriate.

Manager’s Responsibilities

On receiving a phone call reporting your absence, your manager should complete a Record of Notification of Absence form and place it in your personnel record.

During your period of absence your manager will monitor the situation to ensure that sickness reporting procedures are being adhered to. If not, your manager will take appropriate action, which might include telephoning you for a progress report and reminding you of the correct procedure, writing file notes of any conversations and writing to you. As set out above, if you fail to follow the correct procedures you may be subject to disciplinary action and may not receive sick pay.

If you have not telephoned your manager by 10:00am on the first day of absence, your manager will arrange to send a letter to you and your absence will be treated as unauthorised and you will not be paid. If you subsequently confirm that the reason for your absence was due to sickness, your manager will arrange to re-instate their SSP only. Consideration should be given as to whether Healthwatch Kingston Sick Pay should be paid as the employee has failed to adhere to the sickness absence notification procedures.

When you have been signed off work by your General Practitioner and your manager has received certification to support this, you cannot return to work until you have obtained a certificate from your doctor confirming your fitness to resume duties.

On your return, your manager will conduct a ‘Return to Work’ Interview with you. This should happen whatever the duration of your absence. This interview should be carried out in private. Your manager will complete the ‘Return to Work’ form as a record of the conversation and you will be required to sign the form. If you refuse for any reason, this should will be noted on your personnel file. The completed will be placed in your personnel record.

Where possible, Return to Work interviews will be carried out on the day that you return to work.

Your manager should ensure that where appropriate a risk assessment is carried out with the employee prior to them resuming their normal duties.

The Record of Sickness Absence Form should be updated by your manager every time sick leave is taken and the form will be kept in your personnel records.

Sick Pay

All employers are obliged to pay statutory sick pay (SSP) to all eligible employees for periods of absence of three qualifying days or more for a total of 28 weeks in one period of incapacity for work.

The Charity will pay SSP for the first 28 weeks of illness for those employees who qualify for SSP. Your entitlement to SSP depends on:

* the number of days of sickness - there is no entitlement for the first three qualifying days
* proper notification to the Charity of your absence through sickness (which you must do before the end of the first qualifying day)
* provision of medical certificates, i.e. self-certificate sickness form, and, after seven days of illness a doctor's certificate
* you must be over 16
* your contract must be for a period of more than three months
* you must be paid more than the lower earnings limit for National Insurance contributions purposes
* your qualifying days for SSP are those you normally work, e.g. Monday to Friday inclusive

HWK SICK PAY SCHEME

In addition you may qualify for the Healthwatch Kingston (HWK) Sick Pay Scheme. As set out above, payments through this scheme will only be paid if the correct Sickness Absence Procedures are followed.

Sick pay is composed of two parts – SSP and the HWK sick pay. Where payable, HWK sick pay is used to top up SSP, i.e. any SSP will made up to the employees’ basic rate of pay. HWK sick pay will entitle qualifying employees to be paid a maximum of 10 days full pay and 10 days half pay in any 12-month rolling period (i.e. in any 12 month period, an employee will receive 20 days HWK sick pay and no more, irrespective of how many periods, or the length of any period, of sickness absence), under the following circumstances:

* You must be a permanent employee, either full or part time;
* You must have been employed by HWK continuously for 13 weeks;
* The Sickness Absence Procedures must have been following and doctors’ certificates provided as required.

HWK sick pay will not be paid in a case of an accident due to active participation in sport (outside working hours), nor in cases in which the absence arises from or is attributable to, an employee’s own misconduct.

If you are absent from work as a result of an accident and subsequently pursue an insurance claim and receive damages from a third party, HWK reserves the right to recover a refund of the sick pay paid under the HWK sick pay scheme, or a proportion of the sick pay represented in the amount of settlements received.

Payments under the HWK sick pay scheme will usually exceed payments under SSP. However, where you are not entitled to receive HWK sick pay, or that entitlement has been exhausted, payments will be made in accordance with SSP regulations.

SSP and HWK sick pay is paid by HWK through the payroll in the normal way. All payments during sickness absence are regarded as normal pay for the purpose of statutory deductions. Tax and NI will therefore be deducted.

If and when you exhaust your entitlement to HWK sick pay, HWK’s Payroll Provider must be notified.

Flexible Working

The Charity abides by current statutory legislation regarding requests for flexible working arrangements.

We will consider any request to work flexibly against clear criteria and in a consistent way. If you require information about your right to request flexible working, please contact your Manager or an Officer of the Charity who will provide this information to you.

## Parental Leave

All employees who have or expect to have responsibility for a child will be entitled to be absent from work on parental leave for the purpose of caring for that child.

The Charity will at all times comply with the current legislation in force at that time in regard to parental leave.

## Annual Leave

Your annual entitlement will be set out in your contract of employment, the holiday year runs from the 1st January until the 31st December. You will accrue annual holidays on the basis of 1/12th of the annual entitlement for each month of service in the holiday year and holiday entitlement will be accrued by part time employees on a pro rata basis.

**Public Holidays are:**

New Year’s Day Good Friday

Easter Monday May Day Bank Holiday

Spring Bank Holiday Late Summer Bank Holiday

Christmas Day Boxing Day

Holidays are to be taken at times convenient to the Employer and must be requested on an Holiday Leave Request Form obtainable from your Manager who must then sign and authorise your request and you must give the following notice of your intended holiday:

1 day’s holiday – 2 days’ notice

2 days’ holiday - 1 weeks’ notice

3 days up to 5 days’ holiday – 2 weeks’ notice

5 days up to 10 days’ holiday – 4 weeks’ notice

No holiday may be taken during the first 13 weeks of employment, unless agreed before your start date. Holiday entitlement will accrue during this period.

The minimum holiday period that can be taken is one half of a day or the equivalent hours.

More than 10 days holiday to be taken consecutively will only be granted in exceptional circumstances and if appropriate cover for your position can be found. We cannot accept any responsibility for bookings for holidays made before permission is granted for holiday leave.

All holiday entitlement must be taken in the current holiday year and not transferred to any subsequent holiday years.

If you leave our employment payment will be made for any accrued holiday entitlement not taken by you but you may be required to take any accrued holiday during your notice period.

If you leave our employment having taken in excess of your entitled amount of holiday this will be deducted from any salary due if a sufficient amount is owing to you. Any amount in excess of this will be reclaimed from you by way of a debt and will be payable by the termination date of your employment.

If the Charity has terminated or would be entitled to terminate your employment due to misconduct or gross misconduct or if you terminate your employment in breach of this agreement any outstanding holiday pay shall be limited to your statutory entitlement under the Working Time Regulations 1998 and any paid holidays including paid Public holidays taken shall be deemed first to have been taken in satisfaction of that statutory entitlement.

You will not accrue any contractual holiday entitlement during any period of notice for which you are paid in lieu.

## Time Off in Lieu

You may accrue time off in lieu (TOIL) if authorised in advance by your Manager.

TOIL is accrued when hours are worked outside of normal working hours for operational reasons. All accrual of TOIL must be authorised in advance by your Manager.

No more than the equivalent of 50% of normal working hours per week may be accrued. So, for example, if you work 35 hours per week you can accrue no more than 17.5 hours TOIL.

Employees who choose to work outside of normal working hours through personal choice will not accrue TOIL.

TOIL should be taken as soon as is reasonably possible after it has been accrued.

Managers can only authorise TOIL where work needs to be undertaken outside of normal working hours.

If you who have accrued TOIL you should to take this at a time which is operationally viable and without unreasonable delay.

## Time Off for Emergency Leave for Dependants

Employees are entitled to take emergency unpaid time off without pay to attend to a person for whom they have specific caring responsibilities who is their dependant and where those care arrangements have either broken down or where some other emergency has arisen. The leave is given to enable you to put in place further arrangements to cover the care arrangements or to deal with the emergency to enable you to return to work as soon as you are able. If you are late or absent in such circumstances you must report to your Manager at the earliest opportunity. You must also give a likely indication of when you are likely to be able to return to work and this must be as soon as you are able to do so.

The length of the absence must be reasonable in all circumstances. This will depend on the particular instance but we would not normally expect it to exceed one or two days at most. In many cases we would expect leave of half a day or less to be appropriate.

During the period of emergency leave your terms and conditions of employment other than remuneration will continue as if you had not taken emergency leave. Your holiday entitlement will not be affected and will continue to accrue.

## Bereavement

In the unfortunate event of the death of close relatives of an employee, compassionate leave will be allowed at the discretion of your Manager.

The time allowed will depend on the circumstances at the time and will be influenced by the relationship to the employee and travelling times involved.

If an employee requires more time away from work than is allowed as compassionate leave, then holiday entitlement or absence without pay may be agreed with your Manager.

## Disciplinary Procedure

Our disciplinary procedure is carried out according to the current ACAS Code of Practice 1 (the “Code”) and is in place to encourage employees to conform to acceptable standards of discipline at work.

The basis of our procedure is to establish the facts of any situation concerning an employee’s conduct or performance as quickly as possible and to attempt to deal with it as fairly as possible and not to take any action until the facts have been fully investigated.

Before taking any formal action your manager will make every effort to resolve the situation by informal discussion with you. If this hasn’t resolved the situation or it is considered too serious for an informal approach then the formal disciplinary procedure will be followed.

**Formal Disciplinary Procedure**

**Verbal Warning**

If your conduct or performance continues to be unsatisfactory or is considered to be too serious to deal with informally, you will be informed verbally about your unsatisfactory conduct or performance. A meeting in accordance with the Code will be held and a record of any verbal warning will be kept on your personnel record for 12 months and will contain details of the misconduct or performance that resulted in the verbal warning being issued. At the time of issuing a verbal warning you should be aware that a written warning may be issued if there is no sustained satisfactory improvement or change.

**Written Warning**

If your conduct or performance continues to be unsatisfactory or is considered to be too serious for you to be warned verbally a meeting in accordance with the Code will be held and you will be issued with a written warning. This will remain on your personnel record for 12 months and will contain details of the misconduct which resulted in the written warning being issued. At the time of issuing a written warning you will be informed that a final written warning may be issued if there is no sustained, satisfactory improvement or change.

**Final Written Warning**

If the misconduct is serious then a meeting will be arranged in accordance with the Code and you could be issued with a final written warning without first being given a verbal or written warning. At the time of issuing a final written warning you will be informed that your employment may be at risk if there is no sustained satisfactory improvement or change.

**Dismissal for Misconduct**

If any misconduct is considered to be too serious to warrant a warning or if a final written warning has already been issued a disciplinary meeting will be organised to consider an employee’s misconduct and the employee’s employment will be at risk. If you are dismissed for misconduct then you will be entitled to payment in lieu of notice.

Examples of dismissal for misconduct are: (this list is not exhaustive as every circumstance cannot be anticipated): lateness, absence, failure to follow the absence rules and procedure, failure to follow work rules and procedures, breach of work rules, failure to follow a reasonable instruction, inappropriate behaviour, misuse of the Employer’s I.T. and email system and insubordination.

**Dismissal for Gross Misconduct**

If any misconduct is considered to be so serious that a warning will not suffice or a final written warning has been issued a disciplinary meeting will be held in accordance with the Code to consider whether an employee’s misconduct constitutes gross misconduct and the employee’s employment will be at risk of dismissal without notice or payment in lieu.

The following are examples which could constitute gross misconduct (the list is not exhaustive as every circumstance cannot be anticipated): theft, dishonesty, wilful damage to property, wilful misuse of property, serious misuse of the Charity’s I.T. and email system, fraud, breach of security, breach of confidentiality, serious breach of work rules and procedures, breach of health and safety, falsifying your application form, unauthorised absence, persistent lateness, carrying out work without prior consent, attending work under the influence of alcohol or unprescribed and/or illegal drugs, physical violence, threatening behaviour, bullying and gross insubordination.

**Disciplinary Meetings According to ACAS Code of Practice 1**

After investigation, if the Employer is to proceed with a disciplinary meeting, you will be sent a written notice setting out the allegations and any documentary or recorded evidence intended to be relied on at the meeting will usually be included.

Whilst the Employer is investigating any alleged misconduct you could be suspended on your normal rate of pay. Suspension does not imply that a decision has been made you will usually be suspended to allow further investigation.

A meeting will be organised giving you at least 2 full working days’ notice of its time, date and venue.

You will be invited to attend with a representative who will be a qualified trade union representative or current work colleague of your choice. Your representative may ask questions on your behalf and summarise your position but will not be able to answer questions on your behalf.

If you or your representative is unable to attend the first meeting then you will be given an alternative meeting date within a reasonable time of the first meeting and you and your representative should make every effort to attend the alternative meeting as it could be held in your absence if you do not attend.

You are entitled to call witnesses to the meeting if you wish to do so and if they are work colleagues let us know as soon as you can before the meeting and we will arrange for them to be present at the meeting.

If we are intending to call witnesses then you will be provided with their names and any written evidence they have given.

You will be supplied with any written evidence that we intend to rely on before the meeting.

Every endeavour will be made to ensure the meeting is fair and that you have been given the chance to put forward any evidence you wish to be considered by the chairman of the meeting.

Once the meeting has concluded and all parties have put forward their evidence, the chairman will consider the evidence available and make his or her decision which you will be informed of as soon after the meeting as possible.

**Appeal Process**

It is your entitlement to appeal against any formal disciplinary decision including any warnings. If you wish to appeal against any disciplinary decision you must do so within 5 working days or receipt of the disciplinary decision to the chairman of the disciplinary meeting. You must give full written reasons of your appeal at the time of appealing.

An appeal meeting will then be organised and you will be invited in writing to an appeal meeting.

You will be invited to attend with a representative who will be a qualified trade union representative or current work colleague of your choice. Your representative may ask questions on your behalf and summarise your position but will not be able to answer questions on your behalf.

If you or your representative cannot attend the initial appeal meeting then a further meeting will be organised within a reasonable amount of time. You and your representative should endeavour to attend the rearranged appeal meeting as it could be held in your absence if you do not.

After your appeal has been fully considered by the chairman a decision will be made based upon the facts available. You will be notified in writing within a reasonable time of the decision. This decision is final and there is no further recourse to us.

## Grievance Procedure

The Employer operates a grievance procedure according to the ACAS Code of Practice 1 (“the Code”). It is our policy to ensure that employees with a grievance relating to their employment are able to use this procedure to help to resolve grievances as quickly and as fairly as possible.

**Informal Discussions**

If you have a grievance about your employment you should discuss it informally with your manager or an alternative manager if the grievance concerns your manager. Most concerns will be resolved at this stage but if not then you should follow the formal procedure set out below.

**Formal Procedure**

**Stage 1**

Set out your grievance in writing giving full reasons and as much information as you are able and deliver your written grievance to your manager. If your grievance concerns your manager deliver it to an alternative manager.

A meeting will then be organised in accordance with the Code and you will be given at least two working days’ notice of the meeting.

You are entitled to be accompanied by a representative who will be a qualified trade union representative or current work colleague of your choice. If you or your representative are unable to attend this meeting then a second meeting will be organised within a reasonable amount of time. If you fail to attend the second meeting then a decision about your grievance may be made in your absence.

You will be notified of the outcome of the grievance in writing within a reasonable amount of time of the meeting.

**Stage 2 - Appeal**

If you are not satisfied with the response you receive then you should provide full written reasons why you are not satisfied in writing to your manager, who will then invite you to an appeal meeting within a reasonable amount of time of receipt of your grievance.

An appeal meeting will be held in accordance with the Code and you are entitled to be accompanied by a representative who will be a qualified trade union representative or current work colleague of your choice. If you or your representative are unable to attend the appeal meeting then a second meeting will be organised within a reasonable amount of time. If you fail to attend the second appeal meeting then a decision about your grievance may be made in your absence.

Once this appeal meeting has taken place you will be given a written decision within a reasonable amount of time of the meeting. This decision is final and there is no further recourse to us.

## Pensions

Healthwatch Kingston upon Thames is registered with the National Employment Savings Trust (NEST).

NEST is the workplace pension set up by government – see the website at

[http://www.nestpensions.org.uk](http://www.nestpensions.org.uk/).

All employers are required to automatically enrol and make contributions for anyone who: works or usually works in the UK, earns a salary of more than £10,000 a year (in 2017/18) and is at least 22 years old but under the state pension age.

You will be given written notice of the enrolment arrangements within 6 weeks of the commencement of your employment.

The Board’s policy is that qualifying employees be enrolled with NEST after three months of employment with Healthwatch Kingston. New employees can ask, in writing, to be enrolled at an earlier time.

Once enrolled, you are sent a joining pack by NEST which provides full information on the scheme.

You are able to opt out of this pension scheme. The opting out period of one month starts three working days from the date of enrolment. This date can be found on the welcome letter sent by NEST to  newly-enrolled employees. Employees cannot opt out after this period.

The current and planned level of contributions are:

|  |  |  |
| --- | --- | --- |
|   | From April 2018  | From April 2020  |
| Employer  | 2%  | 3%  |
| Employee  | 3%  | 5%  |

Employee contributions are subject to tax relief.

## Retirement

The Charity complies with all of its statutory requirements regarding retirement and in the absence of a set retirement age if you consider you would like to retire for any reason such as you are due to receive an amount of money for this reason from any pension funds you may wish to discuss this with your Manager in the first instance who will then work with you to assist you to achieve your aims.

## Expenses

All reasonable, legitimate and approved expenses incurred by you in the course of your employment will be paid by the Charity. This is subject to you completing an expense claim form, which must be signed by your Manager for authorisation and to the schedule of allowances and authorisation procedures below.

When incurring expenditure of any kind on behalf of Healthwatch Kingston, employees are expected to keep the cost to a minimum at all times.

All expense claims must be made as soon as possible after the expenses were incurred. Any delayed claims may be rejected and claims in excess of two months old may be declined.

Where relevant you should obtain receipts for all legitimates expenses incurred by you in the course of your employment. Non-expenses items such as equipment, stationery etc may not be included as expenses.

Please be aware that certain expenses can incur Income Tax liability in line with HMRC rules.

If you leave the employment of Healthwatch Kingston you must ensure that all expense claims are submitted and authorised prior to your leave date.

Expense claims will be paid with the following month’s salary.

**Schedule of Allowances**

|  |  |
| --- | --- |
| Public transport   | Actual cost of standard rail, bus, coach or taxi. Taxis may only be used in exceptional circumstances for reasons of emergency or personal safety.   |
| Car mileage  | Any employee using their privately-owned car for authorised business purposes may claim the sum of **30p** per mile.  Mileage to and from your home and normal place of work must not be included and the costs of any parking fines or speeding fines will not be re-imbursed.  |

## Season Ticket Loan

Healthwatch Kingston offer a season ticket loan scheme to its employees. Contact your manager for details of the scheme and how to apply.

## Smoking

Smoking is prohibited on and in any Charity premises that are designated no smoking areas and in any Charity vehicles. Smoking is only allowed in designated smoking areas and during official breaks.

If any employee is found smoking in undesignated areas and/or out of official break times, then they will be subjected to the disciplinary procedure. It should be noted that any employee smoking in an undesignated smoking area could render the Charity liable to a criminal charge and fine. Therefore any breach of the smoking policy will be treated as gross misconduct.

## Dress Code

You are expected to dress appropriately for your daily duties.

## Gifts & Bribery

The Charity complies with all of its statutory obligations contained in the Bribery Act 2010 and will not tolerate bribery.

If you are offered any potential gifts from external suppliers or customers you must contact your Manager to seek approval before accepting a gift. You must inform the external supplier or customer of the Charity policy and procedures regarding gifts and bribery.

You should contact your Manager if you wish to offer gifts of any kind to external suppliers or customers. Do not offer any gifts without approval of your Manager.

If you give or receive any gifts without approval from your Manager the matter will be investigated and you may be subject to disciplinary action which could result in the termination of your employment.

If you are aware of unauthorised gifts being offered to or received by any of your colleagues you must report this to your Manager immediately to enable the matter to be investigated.

You should notify your Manager if you receive any gifts that may be offered to you from external suppliers or customers during the course of your employment.

The Charity conducts business honestly, openly and fairly and does not seek to win any business through any form of inducement. This policy will be monitored and reviewed to ensure that is effective in preventing bribery.

## Email, Internet, Information Technology, Software & Mobile Telephony

Employees are required to comply with the e-mail and internet guidelines and understand that misuse or abuse of e-mail and internet systems can lead to discrimination or harassment, revelation of confidential information, copyright infringement, defamation, and the waste of resources and capabilities. This Policy is to ensure compliance with the high professional standards of the Charity.

Information Technology is an important part of our organisation and plays a considerable part in supporting our operational infrastructure. As such it is important that you do not misuse the tools at your disposal. Misuse of Charity Information Technology could cause the business serious harm and employees who do misuse these tools may be subject to disciplinary action which in certain circumstances may result in the termination of their employment.

E-mail users should be aware that e-mails, sent both internally and externally, may be monitored like conventional mail, and recorded. Your e-mails may be accessed at any time. The sending and receipt of personal e-mail is discouraged and should never interfere with nor disrupt the work of users or colleagues.

Users should be aware that breach of this policy or the guidelines may amount to misconduct and may result in disciplinary sanctions in accordance with the disciplinary procedure. A serious breach could lead to dismissal.

E-mail Guidelines:

* Users should be aware that communication by e-mail has the same legal bearing as communication in any other form and consider the potential consequences of their email before transmission.
* E-mail communications, both internal and external are not guaranteed to be private or to arrive at their destination within a given time. The confidentiality note must appear on all external e-mails. If you receive an e-mail in error, inform the sender, and delete the message from the system.
* If an e-mail is received with an attachment, do not open it unless you are satisfied that you know the sender and that the attachment was expected. Viruses are frequently contained in file attachments, which can be sent automatically from an apparently legitimate source.
* E-mails can encourage informality and a lack of discretion. Whilst some informality may be appropriate with internal e-mails, anything sent externally must maintain all professional standards.
* Do not send abusive, threatening or defamatory e-mails, or anything that may in any way harass or discriminate against anyone.
* Do not participate in "chain" letters and do not conceal your identity or falsify e-mails to make them appear to originate from someone else.
* E-mail users should practice good housekeeping and ensure that they regularly read e-mail contained within their in-box and deal with it promptly.
* Deleted and sent items should not be stored unless required for later access.

Internet, Mobile Phones, Smart Phones and Social Networking and Social Media Guidelines:

* Users must not access, view or download any obscene or discriminatory material. Failure to observe this guideline will be considered gross misconduct and result in dismissal.
* Users must restrict their use of the internet to work-related matters during working hours, though reasonable use of the internet facility for personal use is permitted at other times.
* Do not download and/or install software. To do so may introduce a virus or affect the running of the network, and may be a breach of software licence.
* Access to Facebook, Twitter and other similar social networking sites for non-work related purposes is prohibited during working hours. Employees who may wish to access such sites may do so during breaks and only by using their own mobile phones or other similar devices. You cannot access these sites using the Charity’s information technology.
* All employees should be aware that they should not post damaging or libellous comments about the Charity or about its products or its services or employees on Social Networking or Social Media sites, whether using Charity systems and phones or personal systems or phones. Employees may face disciplinary action if they post comments that damage the Charity’s reputation; such disciplinary action could result in dismissal.
* Employees should not divulge personal data on social networking or social media sites. Such information would include but is not limited to giving away information relating to salary, pay rises, bonuses, or disciplinary records.
* The Charity does not plan to monitor personal phone use or personal use of Social Networking and Social Media sites out of working time but will investigate any allegation made regarding employee breaches of this policy which come or are brought to its attention.

Software:

* Software may only be installed with the approval of the IT Manager or a designated person within the IT department.
* This applies to all Charity computers including PCs, laptops and any computing device such as a mobile phone. Failure to observe this policy may result in disciplinary proceedings.

## Monitoring at Work

The Charity reserves the right to read employees’ e-mails and to monitor employees’ use of the internet, both during routine audits of the computer system and in specific cases where a problem relating to excessive and/or unauthorised use is suspected. In addition, the use of CCTV cameras may be made available in certain locations.

The purposes for such monitoring of both are:

* to promote productivity and efficiency
* to ensure there is no unauthorised use of the Charity’s time
* to ensure that all employees are able to operate in a safe and secure work environment
* to ensure that all employees are treated with respect and dignity at work, by discovering and eliminating any material that is capable of amounting to harassment under the terms of the Charity’s anti-harassment policy

Employees should be aware that telephone calls made and received on the Charity’s telephone network may be routinely monitored and recorded to assess employee performance, to ensure customer satisfaction and to check that the use of the telephone system is not being abused.

## Health & Safety

The Charity regards the occupational health, safety and welfare of its employees and of any contracted or temporarily engaged employees to be of paramount importance.

It is our policy, so far as is reasonably practicable, to provide and maintain a working environment that is safe and without risk to health and adequate with regards facilities and your welfare at work and to enlist the active support of all employees in achieving this objective.

It is your responsibility to familiarise yourself with the health & safety statement which is available from your Manager or from the Facilities Manager at Head Office.

The policy is intended to reflect the Charity’s recognition that it has an obligation to set and maintain high standards of health & safety for all its employees, and also, where they may be affected, for customers and the general public.

The following is an outline to the Charity’s objectives for health & safety:

* to promote standards of safety, health and welfare that comply fully with statutory requirements and approved codes of practice and which take into account current developments in the field
* to maintain safe and healthy work places, to operate safe systems of work, and to protect employees, customers and others, including the public, in so far as they come into contact with foreseeable work hazards
* to provide and maintain a safe and healthy working environment for employees with adequate facilities and arrangements for their welfare
* to provide employees with information, instructions and training, and the supervision they require to work safely
* to develop safety awareness and individual responsibility for health and safety of all employees
* to ensure that equipment is constructed, maintained and tested to a standard in accordance with health & safety legislation and other appropriate standards
* to encourage full and effective joint consultation on health & safety matters at all levels of the organisation

For the policy to work effectively your co-operation will be required. An accident book will be kept in each location.

 The duties and accountabilities of each employee therefore are as follows:

* to understand and appreciate that, under the requirements of the relevant legislation, all employees have a duty of care for their health & safety and that of other persons who may be affected by their acts or omissions
* to understand and appreciate that they must also co-operate with management to enable them to comply with any duty placed on them in respect of the above
* To read the Charity’s health & safety policy and any such related documentation that may be relevant to them, as provided by the Charity’s management
* to attend and participate in appropriate training sessions
* to report all accidents/incidents as they occur to the department manager and carry out instructions issued by that person

## Eye Care Policy

The Charity will pay for a standard eyesight test for all permanent employees who use VDU equipment for the majority of their day.

If the test shows glasses are required specifically for VDU use, the cost of a basic pair of frames and lenses will be covered by the Charity. A copy of your prescription will need to be seen by the Charity prior to purchase.

## Lone Working Policy & Personal Security

Your safety is of paramount importance to us. The Board will seek to take appropriate and realistic action to protect the safety of its employees when they are working on their own either in the office or away from the office.

Personal Security

Money and valuables should never be left on display or unattended. The Charity accepts no liability for loss of, or damage to, an employee’s property. In all cases of theft or dishonesty involving property belonging to the Charity, an employee or visitor, the offender will render themselves liable to summary dismissal and prosecution.

In the office –

If you are alone working in the office please use common sense with regard to personal safety. The following procedures will apply -

* A sign will be maintained on the office door at all times that asks callers to knock and then wait for attention. This is to discourage anyone walking into the office without being greeted at the door.
* Whenever there is only one person in the office, the office door will be kept locked and callers will be greeted at the door
* In any situations of threat at the office door, the panic alarm (located on the nearby wall) should immediately be activated
* With the exception of board members and known employees of other organisations, anyone working alone in the office must not meet visitors in the office. Instead, they may meet them somewhere in the building that is visible to other users of the Centre. If this is difficult to arrange, then another time should be arranged for the meeting.

An Incident Book will be maintained in the office in which staff should record any circumstances raising concern. Any entries will be reported to a Board member as soon as possible for review and may be discussed with the management of the Kingston Quaker Centre so that any suitable preventative action can be identified and carried out.

Out of the office -

* Any employee leaving the office for a meeting should inform their line manager or a colleague where they are going, who they are meeting with, their contact details and at what time they expect to return (or if they do not intend to return because it is the end of the working day). If there is no member of staff available to inform, written details should be left visible on a suitable desk in the office.
* Meetings with individuals must be held in venues that are visible to the public.
* If it is necessary, for a meeting to take place in someone’s home, the meeting must be attended by two members of staff.

## Right of Search

Although we do not have the contractual right to carry out searches of employees and their property whilst they are on our premises, we would ask all employees to assist us in this matter should we feel that such a search is necessary. Any such search does not imply suspicion in relation to any individual concerned.

If you should be required to submit to a search, if practicable you will be entitled to be accompanied by a third party to be selected from only someone who is on the premises at the time a search is taking place.

## Charity Property

Charity property is not intended for private use. Reasonable private use of Charity property may be allowed, but if this use is excessive then the matter will be investigated and may result in disciplinary action being taken. This could ultimately result in dismissal. You are advised to seek approval from your Manager.

 The following is a list of examples of Charity property, this list is not exhaustive:

* telephones
* computers
* stationery supplies
* mobile phones
* charity vehicles
* charity credit cards

If equipment belonging to the Charity has been installed at your home you must ensure that it is not damaged in any way. If it is stolen you must notify us immediately. You may be required to reimburse the costs if the loss was a direct result of your negligence.

If it is considered that the equipment no longer needs to be at your home, or if your employment is terminated, then you will be required to return it immediately, if a phone line is connected this will be cut off when you leave the Charity.

If you fail to return any Charity property when your employment is terminated the cost of replacing such Charity property will be deducted from any sum owed to you by the Charity.

## Protected Disclosures

The Charity actively encourages workers/employees to disclose any concerns about wrong-doing within the Charity. Wrong-doing within the Charity may amount to one or more of the following matters that has occurred, is occurring or is likely to occur in the future:

* a criminal offence
* breach of a legal obligation
* miscarriage of justice
* a danger to the health and safety of any individual
* damage to the environment
* deliberate cover-up of any of the above matters
* damage to the reputation of the Charity as a result of damaging or libellous comments being posted on social networking or social media sites
* bullying, harassment or victimisation of an employee via cyber bullying and/or social networking or social media sites

Where you have a concern in terms of any of the above examples you should immediately report any allegations or concerns about malpractice to your Manager or an Officer of the Charity.

Any information you provide will be treated in the strictest confidence. You will be kept informed of the progress of the Charity’s investigation into the alleged malpractice and the steps which will be taken upon the conclusion of the Charity’s investigations.

Provided you raise your concerns in good faith regardless of whether or not it is ultimately substantiated, no disciplinary action will be taken against you by the Charity.

Where your allegation or concern is communicated by you to an external source before you have exhausted the internal procedure set out, this may result in disciplinary action being taken against you if it is considered that your act in communicating your allegation to an external source was unreasonable before attempting to resolve it internally.

## Anti-Slavery Policy

**Statement**

This statement is in accordance with the Modern Day Slavery & Trafficking Act 2015.

Modern slavery is a crime and a violation of fundamental human rights. It takes various forms, such as slavery, servitude, forced and compulsory labour and human trafficking, all of which have in common the deprivation of a person's liberty by another in order to exploit them for personal or commercial gain.

Kingston Healthwatch has a zero-tolerance approach to modern slavery and we are committed to acting ethically and with integrity in all our business dealings and relationships and to implementing and enforcing effective systems and controls to ensure modern slavery is not taking place anywhere in our own business or in any of our supply chains.

We are also committed to ensuring there is transparency in our own business and in our approach to dealing with our responsibility to eradicate modern slavery throughout our supply chains.

We expect the same high standards from all of our contractors, suppliers and other business partners and will abide by our responsibility to ensure that those we deal with exercise prohibitions against the use of forced, compulsory or trafficked labour, or anyone held in slavery or servitude, whether adults or children, and we expect that our suppliers will hold their own suppliers to the same high standards.

This policy applies to all persons working for Kingston Healthwatch or on our behalf in any capacity, including employees at all levels, Officers, contractors, suppliers, external consultants, third-party representatives and business partners.

**Responsibility for the policy**

* The Charity’s Officers have overall responsibility for ensuring this policy complies with our legal and ethical obligations, and that all those under our control comply with it.
* The Chief Officer has primary and day-to-day responsibility for implementing this policy, monitoring its use and effectiveness, dealing with any queries about it, and auditing internal control systems and procedures to ensure they are effective in countering modern slavery.
* Management at all levels are responsible for ensuring those reporting to them understand and comply with this policy and are given adequate and regular training on it and the issue of modern slavery in supply chains.
* You are invited to comment on this policy and suggest ways in which it might be improved. Comments, suggestions and queries are encouraged and should be addressed to the Chief Officer.

**Compliance with the policy**

* You must ensure that you read, understand and comply with this policy.
* The prevention, detection and reporting of modern slavery in any part of our business or supply chains is the responsibility of all those working for us or under our control. You are required to avoid any activity that might lead to, or suggest, a breach of this policy.
* You must notify your manager OR the Chief Officer as soon as possible if you believe or suspect that a conflict with this policy has occurred or may occur in the future.
* You are encouraged to raise concerns about any issue or suspicion of modern slavery in any parts of our business or supply chains of any supplier tier at the earliest possible stage.
* If you believe or suspect a breach of this policy has occurred or that it may occur you must notify your manager or the Chief Officer OR report it in accordance with our Protected Disclosure (Whistleblowing) Policy as soon as possible.
* If you are unsure about whether a particular act, the treatment of workers more generally, or their working conditions within any tier of our supply chains constitutes any of the various forms of modern slavery, raise it with your line manager or the Chief Officer.
* We aim to encourage openness and will support anyone who raises genuine concerns in good faith under this policy, even if they turn out to be mistaken. We are committed to ensuring no one suffers any detrimental treatment as a result of reporting in good faith their suspicion that modern slavery of whatever form is or may be taking place in any part of our own business or in any of our supply chains. Detrimental treatment includes dismissal, disciplinary action, threats or other unfavourable treatment connected with raising a concern.
* If you believe that you have suffered any such treatment, you should inform your line manager immediately. If the matter is not remedied, and you are an employee, you should raise it formally using our Grievance Procedure, which can be found in the current employee handbook.

Breaches of this policy

Any employee who breaches this policy will face disciplinary action, which could result in dismissal for misconduct or gross misconduct.

We may terminate our relationship with other individuals and organisations working on our behalf if they breach this policy.

**Confirmation of Receipt – Kingston Healthwatch Employee Handbook**

I confirm that I have received and read the Kingston Healthwatch Employee Handbook and agree to comply with the conditions contained within it.

Signature:

Name:

Date: