Data Protection – Breach Reporting Policy

General

This policy forms part of the company's suite of data protection policies. It is drafted so as to comply with the GDPR (General Data Protection Regulation) which comes into force in England on the 25th May 2018 and which replaces the Data Protection Act 1998.

This policy is to be read by any employee who is authorised and instructed to prepare breach report forms.

The appendices attached to the policy form part of the policy.

In the event of any query, employees tasked with preparing a breach report form should contact **Phill Hutchinson Data Protection Officer (DPO)**

Further information about some of the terms used in this policy (such as what constitutes a data controller or what constitutes personal data) can be found in the Headline Data Protection Policy.

This policy confirms the legal framework applicable to data protection breaches and the steps that we must take in order to deal with any such breach.

Legal Framework

The GPDR imposes positive obligations on data controllers to document and, where necessary, report breaches of data protection legislation.

There are no limits to the circumstances which might constitute a data protection breach. Common situations include accidental loss of data, deliberate hacking, use of personal data otherwise than pursuant to a Privacy Statement and other breaches of data protection legislation.

All breaches of data protection must be reported and recorded. Where a breach is such that there is a high risk that an individual's rights and freedoms will be affected, the individuals must be notified of the breach and the steps that we are taking to remedy the breach.

Where it is likely that there will be a risk to people's rights and freedoms as a result of a data protection breach, the breach must also be reported to the Information Commissioner's Office (ICO).

Breaches must be reported to the ICO no more than 72 hours after we become aware of the breach.

Responsibility for Breach Reporting

It is the responsibility of the company's Data Protection Compliance Officer ("DPO") to deal with data protection breaches pursuant to this policy. Where we are obliged by law to appoint a data protection officer, that person will be the DCPO for the purposes of this policy.

In the event of a breach, it is the responsibility of the DCPO to complete the breach report form, take any corrective actions which are deemed necessary and to make any onward reports, either to the individuals affected or to the ICO.

Where the DCPO (Phill Hutchinson) is not available, responsibility for ensuring compliance with this policy falls to the deputy DCPO, Antony Pearson. If the deputy DCPO authorises another employee to carry out the functions of the DCPO under this procedure, that authorisation must be provided in writing and a copy of the authorisation appended to the breach report form.

Deputy DCPO will also be responsible for ensuring that any employee other than the DCPO who is authorised to complete this report has completed it correctly and must approve any decision to report or not report to the ICO or to the individuals affected.

In any situation where someone other than the DCPO has completed the breach report form, the DCPO must be notified of the breach report as soon as they are available. In that situation, the DCPO has authority to overturn any decision taken by any other officer or employee.

General Responsibilities of All Employees

Every employee of the company and every other worker or contractor who is obliged to comply with the provisions of this policy has personal responsibility to:-

1. Minimise the possibility of any breach of the company's data protection procedures; and

2. Promptly report any breach which comes to their attention to the DCPO or, in the absence of the DCPO, to the deputy DCPO; and

3. Immediately report any breach of this policy occasioned as a result of the individual's own acts or omissions to the DCPO or, in the absence of the DCPO, to the deputy DCPO.

Although the company reserves the right to take appropriate action (which, in the case of employees, may be action pursuant to the company's disciplinary procedure) against individuals who are responsible for data protection breaches, the company will usually only take such action where it is considered that the breach is so serious or the actions leading to the breach were so negligent or wilful that such action is appropriate.
In most cases (and to ensure transparency in reporting), the company will not take any action against the individual other than in respect of highlighting corrective actions or highlighting (and dealing with) training needs.

As such, all individuals are actively encouraged to report their own breaches of data protection without fear that they will be subject to any sanction as a result.

Failure to report a breach (whether occasioned by an individual or whether occasioned by a third party known to the individual) will be seen as behaviour warranting disciplinary action in the case of employees and potential termination of engagements in the case of workers and contractors.

The company does not routinely conduct spot checks. The company reviews matters following all Breach Report to ensure that it's policies and procedures are operating correctly and are compliant and will make changes where this is found to be necessary

Breach Report Register

The DCPO maintains a register of all breach reports, including those which are not reported to affected individuals and/or the ICO.

Each breach report is numbered sequentially and must be kept in the central register.

Completing a Breach Report Form

All data protection breaches must be reported using the company's breach report form.

The breach report form will be updated from time to time to ensure that it remains compliant with data protection legislation.
The breach report form must be completed in full in order to ensure compliance with data protection legislation.

The Reporting Employee named on the breach report form is the individual completing the breach report form. This will usually be the DCPO unless the DCPO is not available, in which case it will be the individual appointed pursuant to this policy.

At section 3 of the breach report form, the Reporting Employee must give as much information as possible about what has happened, when it happened and how it happened. Where there has been any attempt to hide the breach, full details of that must be given.

Where there is insufficient space on the form to set out all of the details, the details should be typed on a separate sheet which is endorsed with the breach number and then affixed to the breach report form.

The purpose of section 3 is to ensure that the DCPO (if someone other than the DCPO was the Reporting Employee) and/or the ICO and/or any other person lawfully entitled to review breach report forms and/or the directors of the company are able to see precisely what has happened and form an immediate view as to whether the right action has been taken by the company.

At section 4, the Reporting Employee should think about how many individuals will be affected as a result of what has happened. For example, if an e-mail has been sent to the wrong recipient and only contains information about one person, this will be easy to answer. If bulk data has gone missing or has been abstracted, try and provide the best estimate of the number of individuals affected by the breach. This section is not about the severity of the breach – it is simply a record of the number of people who the company believes will be affected by the breach.

Section 5 relates to the likely consequences of the breach. The Reporting Employee is encouraged to look at all possible consequences of the breach and should not minimise the likely consequences either to protect the company or to justify not making a report to the individuals affected and/or to the ICO. In many situations, it may not be possible to say with any certainty what may happen, but where data is in the hands of a third party who has no right to have it and there is no realistic possibility that that person can be prevailed upon to return the data and/or destroy any data which is in their possession, regard should be had to the possibility that data could be used for (for example) identity theft or other types of fraud.

Where the data is improperly in the hands of a third party whom is known to the company and who may have a contractual, professional or other relationship to the company, the likely consequences of the breach may be rather less serious.

Reporting a Breach

Where the consequences of the breach are likely to lead to a high risk that the rights and freedoms of the affected individuals will be adversely affected, those individuals must be notified of the breach.

Similar considerations apply when deciding whether or not a breach should be reported to the ICO. Where it is decided not to report to either the affected individuals or the ICO, the "internal report" box in section 6 can be ticked. In that situation, the reasons why it is not felt that an external report to either the affected individuals or the ICO is necessary should be recorded in the "further comments" section at section 8 of the form.

Where a breach is regarded as sufficiently serious to warrant a report to the affected individuals and/or the ICO, the relevant boxes should be ticked and details of the breach be provided to the person to whom it is to be disclosed, together with details of the corrective actions to be taken and the dates on which those actions will be taken.
In every case, whether or not there is an external report to the individuals affected and/or the ICO, the Reporting Employee should set out the corrective actions which are to be taken to deal with the breach that has been identified and to prevent such breaches happening in the future. Dates by which actions should be taken must be included and it will be the responsibility of the DCPO (or such person acting in lieu of the DCPO) to ensure that these dates are met.

Corrective actions might include steps taken to remedy the immediate breach and recover any information which has been improperly disclosed or might involve reporting thefts to the police as well as to the ICO. Corrective actions to prevent a recurrence of a breach might include identifying trends in breach reporting (to see if there is any weakness in the company's procedures which is leading to breaches) or individual training requirements for employees who are responsible for the breach. Where the breach is occasioned as a result of repeated failure to abide by the company's data protection procedures, most widespread training may be necessary and where such refusals to abide by the company's data protection procedures are noted, formal disciplinary action may also be required against the employees concerned.

Policy Approved by Phill Hutchinson/Sue Callon

Name:	
Job Title:	
Manager:	

I confirm I have read and understood the Hollow Oak Nursing Home Ltd

Data Protection – Breach Reporting Policy

I also confirm that I have sought clarification from my Manager on any issues outlined in the Policy which I am not clear about.

Signed: _____

Date: _____

Please return this form duly completed and signed to your Manager.