DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: Caerphilly County Borough Council/
Cyngor Bwrdeistref Sirol Caerffili

Penallta House
Tredomen Park
Ystradmynach
Hengoed
Mid Glamorgan
CF82 7PG

I, Chris Burns, Interim Chief Executive of Caerphilly County Borough Council hereby acknowledge the details set out below and undertake to comply with the terms of the following Undertaking:

1. Caerphilly County Borough Council is the data controller as defined in section 1(1) of the Data Protection Act 1998 (the 'Act'), in respect of the processing of personal data carried out by Caerphilly County Borough Council and is referred to in this Undertaking as the 'data controller'. Section 4(4) of the Act provides that, subject to section 27(1) of the Act, it is the duty of a data controller to comply with the data protection principles in relation to all personal data in respect of which it is a data controller.

2. The Information Commissioner (the 'Commissioner') received a data breach notification on 28 November 2013 relating to covert surveillance which had been undertaken on an employee suspected of defrauding the data controller in breach of the sickness absence policy.

3. The Commissioner accepts that the use of covert surveillance to monitor employee behaviour can be justified in some circumstances. However, as set out in s.3.4.1 of the Commissioner's Employment Code of Practice, in order to justify such action the employer must be satisfied that there are grounds for suspecting criminal activity or equivalent malpractice, and that notifying individuals about the monitoring would prejudice its prevention or detection. Abuses of an organisation's sickness policies can amount to such malpractice, but covert surveillance should only be used in exceptional circumstances as a last resort when alternatives which respect the employee's privacy have been considered and are not viable/ appropriate.

4. On the specific facts of this case the Commissioner does not consider that the data controller had sufficient evidence to warrant the authorisation of covert surveillance on an employee. In this case the employee had only been off work with a sick note for anxiety and stress for four weeks at the time the surveillance was authorised. The surveillance was authorised on the basis that the employee had told a few people that she felt housebound and the data controller believed the employee would use the absence to avoid attending meetings she was required to attend at work.

5. However there was no medical indication that the employee was housebound and no other measures were taken to discuss the employee's sickness absence and potential attendance at meetings before resorting to covert surveillance at such an early stage. The data controller has accepted that there had been no evidence to suggest that the employee would use the sickness policy as a basis for not attending the meetings she was required to attend. In fact the employee attended a meeting which took place shortly after the surveillance had been carried out without being aware that the surveillance had been conducted.

6. The data controller has also confirmed that the report which was produced by the surveillance company was never used. This was despite the report verifying that the employee was not housebound.

7. Given the above it is the Commissioner's view that there were not sufficient grounds at this early stage of the employee's sickness absence to justify the authorisation of covert surveillance. The Commissioner therefore considers that the covert surveillance of the employee's activities was unfair and in breach of the First Data Protection Principle which is set out in Schedule 1 Part I to the Act.

8. In consideration of the Commissioner not exercising his powers to serve an Enforcement Notice under section 40 of the Act, after he has taken into account the data controller's suspension of the covert surveillance of employees pending a review, the data controller undertakes as follows:

The data controller shall, as from the date of this Undertaking and for so long as similar standards are required by the Act or other successor legislation, ensure that personal data are processed in accordance with the First Data Protection Principle in Part I of Schedule 1 to the Act, and, in particular:

(1) Follow the ICO's Employment Practices Code (available at http://ico.org.uk/for_organisations/data_protection/topic_guides/employment) when reviewing the employee surveillance policies, procedures, guidance and training, and conducting any covert surveillance in the future.

(2) In particular follow the guidance provided in section 3 of the ICO's Employment Practices code covering the use of impact assessments and covert monitoring which includes the following guidance in particular:

Impact Assessments

In order to ascertain whether covert surveillance could be justified the data controller should conduct an impact assessment to determine whether the adverse impact on the employee(s) is justified by the benefits to the employer and others. This is to ensure that any covert surveillance is a proportionate response to the problem it seeks to address.

Such an impact assessment must:

- clearly identify the purpose(s) behind the surveillance and the benefits it is likely to deliver,
- identify any likely adverse impact of the surveillance,
- consider alternatives to surveillance or different ways in which it can be carried out,
- take into account the obligations that arise from the surveillance, and
- judge whether the surveillance is justified.

Covert Monitoring:

- Senior management should authorise any covert monitoring. In doing so they must satisfy themselves that there are grounds for suspecting criminal activity or equivalent malpractice (i.e. serious but non-criminal employee misbehaviour such as fraudulently claiming sick pay) and that notifying individuals about the monitoring would prejudice its prevention or detection. Such covert monitoring should only be used in exceptional circumstances as it will be rare for covert

monitoring of employees to be justified.

- Ensure that any covert monitoring is strictly targeted at obtaining evidence within a set timeframe and that the covert monitoring does not continue after the investigation is complete.

- Do not use covert audio or video monitoring in areas which workers would genuinely and reasonably expect to be private.

- If a private investigator is employed to collect information on workers covertly make sure there is a contract in place that requires the private investigator to only collect information in a way that satisfies the employer's obligations under the Act. Check any arrangements for employing private investigators to ensure your contracts with them impose requirements on the investigator to only collect and use information on workers in accordance with your instructions and to keep the information secure.

- Ensure that information obtained through covert monitoring is used only for the prevention or detection of criminal activity or equivalent malpractice. Disregard and, where feasible, delete other information collected in the course of monitoring unless it reveals information that no employer could reasonably be expected to ignore.

(3) Ensure that in every case an appropriate written impact assessment is completed.

Signed: …….

Chris Burns
Interim Chief Executive
Caerphilly County Borough Council

Dated: …….

Signed: …….

Stephen Eckersley
Head of Enforcement
For and on behalf of the Information Commissioner

Dated: …….