Data Protection Act 1998
Undertaking follow-up

Flybe Limited
ICO Reference: COM0561828

On 1 April 2016 the Information Commissioner's Office (ICO) conducted a follow-up assessment of the actions taken by Flybe Limited in relation to the undertaking it signed on 16 February 2015.

The objective of the follow-up is to provide the ICO with a level of assurance that the agreed undertaking requirements have been appropriately implemented. We believe that appropriate implementation of the undertaking requirements will mitigate the identified risks and support compliance with the Data Protection Act 1998 (DPA).

The follow-up assessment consisted of a desk based review of the documentary evidence Flybe Limited supplied to demonstrate the action it had taken in respect of the undertaking requirements. This included: the information security and handling policy, information handling quick reference guide for staff, membership certificate for the information security forum (ISF), ISF information security audit, training and policy completion statistics, information asset register, whistle-blowing policy, Audit Committee Report and a weekly Executive Committee update .

The review demonstrated that Flybe Limited has taken appropriate steps and put plans in place to address the requirements of the undertaking and to mitigate the risks highlighted.

Flybe Limited confirmed that it has taken the following steps:

- Revised the information security and handling policy.
- Produced a quick reference guide for staff on the information security and handling policy, which is given to staff at induction.
- An information security training video is shown to all members of staff at induction.
- Implemented information security e-learning training which requires a pass mark of 80%.
- Training completion statistics are reported to the Executive Committee as well as statistics for how many staff have read and understood the information security and handling policy.
- All "high risk" roles have had specific data protection training provided by an external DPA specialist.
- Staff that access highly confidential and sensitive personal data are given training prior to being granted access to personal data.

- All staff members who will require access to highly confidential, personally sensitive data require enhanced background checks.
- The information asset register has been developed which assists with system access controls.
- The whistle blowing policy has been relaunched to encourage employees to report security incidents confidentially.
- Flybe Limited have become members of the ISF and ISF have carried out an information security health check.
- The Audit Committee are regularly updated on plans to improve Flybe Limited's information and cyber security resilience.
- A weekly report is sent to the Executive Committee with information about: cyber security, information security, physical security, people security, detection and prevention, systems review, supplier audit, crisis management and awareness campaigns.

However Flybe Limited should:

- Ensure that all employees that access personal data complete information security training and read the related policies, before they are given access to personal data.
- Display their new data protection awareness posters, as planned.
- To roll out the DPA e-learning module, as planned.

Date issued: 5 April 2016

The matters arising in this report are only those that came to our attention during the course of the follow up and are not necessarily a comprehensive statement of all the areas requiring improvement.

The responsibility for ensuring that there are adequate risk management, governance and internal control arrangements in place rests with the management of Flybe Limited.
We take all reasonable care to ensure that our Undertaking follow up report is fair and accurate but cannot accept any liability to any person or organisation, including any third party, for any loss or damage suffered or costs incurred by it arising out of, or in connection with, the use of this report, however such loss or damage is caused. We cannot accept liability for loss occasioned to any person or organisation, including any third party, acting or refraining from acting as a result of any information contained in this report.