



Abridged Data Privacy Policy

This document articulates operational and performance guidance for Northgate Information Solutions companies, employees and business partners.

This Policy does not create any contractual rights of any kind between Northgate and its employees. In addition, all employees should understand that this Policy does not modify their employment relationship, whether at will or governed by contract. This Policy is inapplicable to the extent voided or restricted by local law. In the event of discrepancy between a local translation and the English version, the English version will prevail.

	INFORMATION
Document Id	Abridged Data Privacy Policy
Document Owner	Harold Babbit
Issue Date	March 2013
Last Saved Date	November 2014

Introduction

An essential activity within the Northgate Group of companies is the requirement to gather and process information about its staff and its customer's staff, in order to operate effectively. This will be done in accordance with the data protection or data privacy laws of the country in which we operate.

The English law version of the 'Data Protection Act' 1998 (the 'DPA') (the 'Act'), should be observed as best practice in countries where there is no equivalent to Data Privacy regulations or laws.

Below are the key points of policy; however the Group Data Protection Policy and a summary of the data privacy laws for the countries in which we operate can be found on the [Group's intranet site](#).

Additional protection is required for health or social service 'patient identifiable information' and for any government information that is protectively marked.

1. Our Responsibility

Northgate, when acting as custodian of personal data, has a legal and contractual duty to ensure that it is handled properly and confidentially at all times, irrespective of whether it is held on paper, processor, memory stick or by any other electronic means. This covers the whole lifecycle, including:

- The obtaining of personal data;
- The storage and security of personal data;
- The use of personal data; and
- The disposal/destruction of personal data.

Northgate also has a responsibility to ensure that data subjects have appropriate access, upon written request to the data controller, to details regarding personal information relating to them.

2. Data Privacy Terms

- **Data Privacy** relates only to living individuals and the most commonly used phrases are 'Personally Identifiable Information' (in the US - often written as PII) and 'Personal Data' (in UK and EU).
- **PII and Personal Data** is information that can be used to identify an individual. Usually it is their name, date of birth, social security number, biometric records, etc...
- **Sensitive Data** goes a step further and is information that includes personal data relating to the data subject's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition, sexual life, alleged commission of any offence, or any criminal history.
- **The Data Subject** is an individual who is the subject of personal data.
- **The Data Controller** is the person/entity who owns and controls personal data, usually an employer. This person/entity is responsible for ensuring secure processing of the data, and must register with

the local Data Protection Agency or Authority. Northgate is the Data Controller for any information we hold as a result of directly doing business (e.g. our own employee's HR and payroll records) and our clients are typically the data controller for any information we process on their behalf.

- **The Data Processor** is any person or entity (other than an employee of the data controller) who processes the data on behalf of the data controller. Northgate is a Data Processor in respect of its client's data where for example it processes payroll on their behalf.
- **A Data Exporter** is a data processor who transfers the data outside of the European Economic Area (EEA).
- Northgate is a Data Exporter when it off-shores work, for example from UK to India or the Philippines.
- **A Data Importer** is a Data Processor who receives the data from the Data Exporter for further processing. For example, someone in Manila is the importer if receiving from Belgium.

3. Data Privacy Principles

Data being processed by Northgate should be:

1. Fairly and lawfully processed;
2. Obtained and processed for specified and lawful purposes;
3. Adequate, relevant and not excessive;
4. Accurate and up to date;
5. Held no longer than necessary;
6. Processed in accordance with the rights of the data subjects;
7. Kept secure; and
8. Not transferred outside of the EEA without adequate data protection safeguards being in place in the country to which it is being transferred.

It should also be noted that data can only be processed where one of the following conditions has been satisfied:

- The individual has given consent to the processing of his/her data;
- The processing is necessary for the performance of a contract with the individual;
- The processing is required under a legal obligation;
- The processing is necessary to protect the vital interests of an individual or to carry out public functions; and
- The processing is necessary to pursue the legitimate interests of the business (unless they are prejudicial to the interests of the individual).

Northgate should ensure that all contracts and service level agreements ('SLA') between Northgate and third parties (including contract staff), which contain provisions for the processing of personal data, make reference to the Act as appropriate.

Northgate should provide all staff (including contractors) only the minimum of privileged access to personal information commensurate to performing their job responsibilities.

Furthermore, Northgate should train all staff (including contract staff) acting on Northgate's behalf to understand their responsibilities under the DPA.

4. Security/Privacy Incidents

Incidents involving exposure of PII or Personal Data can be harmful to our clients and their employees and can result in significant fines, but most importantly for Northgate it could significantly damage its reputation resulting in loss of revenue or potential new customers.

If, despite the security measures we take to protect the personal data we hold, a security incident occurs, it is important to deal with it effectively. The incident may arise from a theft, a deliberate attack on our systems, the unauthorized use of personal data by a member of staff, accidental loss, or equipment failure. In the event of an incident or suspected incident, please inform your manager, the Information Security Officer, or the Whistle-Blowing Hotline immediately and log the incident.

However the incident occurs, management must respond to and manage the incident appropriately. We have a strategy for dealing with an incident that includes the following:

- a recovery plan, including damage limitation;
- conducting an assessment of the risks associated with the incident;
- informing the appropriate people and organizations that the incident has occurred; and
- reviewing our response and updating our information security procedures.

Northgate has a Chief Compliance and Privacy Officer who is responsible for gathering and disseminating information and issues relating to information security, the Data Protection Act and other related legislation.

Northgate has a Data Protection Steering Committee (DPSG), which consists of representatives from all divisions of the Group and legal representatives from each of the four geographical regions (UK, EMEA, US and APJ). The DPSG members act as the point of contact for all communications and issues relating to information security, Data Privacy, and other related legislation within their region.

5. How to raise a concern

- If you have any doubt or concern about any situation relating to the policy, seek guidance from your manager before doing, or omitting to do, anything that could compromise your position.
- If you become aware of any security or data privacy incident, email informationsecuritymanager@northgate-is.com; you can also submit a security incident using Service Now (S-NOW) by checking the 'Security Incident' field.
- You may also use the Whistle Blowing Hotline: whistle-blowing@northgate-is.com.
- If any manager should require further guidance on complying with this policy, please contact a member of the DPSG under data.protection.group@ngahr.com.