Northgate Association Information Security Policy, May 2025

Purpose

Information that is collected, analysed, stored, communicated and reported upon may be subject to theft, misuse, loss and corruption. Information may be put at risk by poor education and training, and the breach of security controls.

Information security incidents can give rise to financial loss, non-compliance with standards and legislation, as well as possible judgements being made against Northgate Association.

This high level Information Security Policy sits alongside the Data Protection Policy. This is to provide the high-level outline of, and justification for, Northgate Association risk-based information security controls.

Objectives

Northgate Association (PTA) security objectives are that:

- our information risks are identified, managed and treated according to an agreed risk tolerance;
- our authorised users can securely access and share information in order to perform their roles;
- our physical, procedural and technical controls balance user experience and security;
- our legal obligations relating to information security are met;
- individuals accessing our information are aware of their information security responsibilities;
- incidents affecting our information assets are resolved and learnt from to improve our controls.

Scope

The Information Security Policy and its supporting controls, processes and procedures apply to all information used at Northgate Association, in all formats. This includes information processed by other organisations in their dealings with Northgate Association.

The Information Security Policy and its supporting controls, processes and procedures apply to all individuals who have access to Northgate Association information and technologies. This includes external parties that provide information processing services to Northgate Association.

For the avoidance of doubt, Northgate Association are a registered charity and are defined under GDPR as the data processor of information. Northgate Primary School is defined as the Data Controller.

Compliance monitoring

Compliance with the controls in this policy will be monitored by the Trustees, and reported to the School aforementioned and the Schools Governers, should this be required.

DATE: Revised June 2023

Review

A review of this policy will be undertaken by the Chair or in their absence the Treasurer. This will be annually or as required.

Policy Statement

It is Northgate Association's policy to ensure that information is protected from a loss of:

- confidentiality – information will be accessible only to authorised individuals (Trustees and Committee Members);
- integrity – the accuracy and completeness of information will be maintained;
- availability – information will be accessible to authorised users and processes when required.

1. Information security policies

A set of lower-level controls, processes and procedures for information security is defined below.

Storage

Northgate Association have acquired a Google Domain (northgatePTA), which is used alongside a Google for Business Account.

- All documentation including not limited to;
- Personal data of Parents, Carers and Children of the School
- Commercial business documentation (risk assessment, insurances, food ratings)
- PTA operational documentation
- Banking & financial documentation
- The above information is used specifically to facilitate the role of a PTA School charity, and is filed in the Google for Business drive and email accounts.

Access

All documentation stored on Google for Business is accessed by Trustees only, using Google domain email accounts.

In some instances, documentation pertaining no personal or confidential business information is shared (for example an event FAQ document) to the School community. The sharing of this document is restricted to those with access to the link.

Equipment

Due to the nature of this charitable business, the Northgate Association Trustees and Committee Members will utilise personal laptops, devices and mobile phones to carry out their duties. However only the Chair and Treasurer have access to the Google for Business drive. And personal and business information is only stored on this drive.

2. Organisation of information security

Northgate Association has implemented suitable governance arrangements for the management of information security. This will include identification and allocation of security responsibilities, to initiate and control the implementation and operation of information security.

Northgate Association will appoint:

- The Chair and Treasurer Trustees to take accountability for information risk
- The aforementioned Trustees will influence, oversee and promote the effective management of information

3. Access control

Access to all information will be controlled aforementioned in section 1 and will be driven by business requirements. Access will be granted or arrangements made for users according to their role and the classification of information, only to a level that will allow them to carry out their duties.

A formal user registration and de-registration procedure will be maintained for access to all information systems and services. This will include methods based on the sensitivity of the information being accessed, and will include consideration of multiple factors as appropriate.

Specific controls will be implemented for users with elevated privileges, to reduce the risk of negligent or deliberate system misuse. The separation of duties will be implemented, where practical.

4. Supplier relationships

Northgate Association information security requirements will be considered when establishing relationships with suppliers, to ensure that assets accessible to suppliers are protected.

Supplier activity will be monitored and audited according to the value of the assets and the associated risks.

At present no Supplier has access to Northgate Association information. Suppliers used to obtain information from Parents, Carers and Children at the School, are for ticket purchasing and volunteer sign up only. The data held is deleted within a month of the event closing.

5. Information security incident management

Guidance will be available on what constitutes an information security incident and how this should be reported. Actual or suspected breaches of information security must be reported and will be investigated. The appropriate action to correct the breach will be taken, and any learning built into controls.

6. Compliance

The design, operation, use and management of information systems must comply with all statutory, regulatory and contractual security requirements.

Currently this includes:

- data protection legislation
- the payment card industry standard (PCI-DSS)

- Northgate Association contractual commitments

Northgate Association will use internal audits to demonstrate compliance against chosen standards and best practice,

This will include:

- IT health checks
- gap analyses against documented standards
- internal checks on staff compliance
- returns from Information Asset Owners

This policy will be reviewed annually by the Northgate Association committee.

Agreed and signed by:

Geri Wren

Chair of Northgate Association

Northgate Association, Registered charity number 1123024 (England and Wales)