Ponteland High School

Data Security Policy

Issue Date May 2018
Last review date January 2020

Introduction

Ponteland High School is committed to maintaining the confidentiality of its information and ensuring that the details of the finances, operations and individuals within the school are protected.

The school recognises, however, that any organisation can be subject to breaches of security particularly given the amount of information that is stored online or on electronic devices which are increasingly vulnerable to cyber-attacks.

This being the case, it is necessary to have a contingency plan containing procedures to minimise the potential negative impacts of any security breach, to alert the relevant authorities, and to take steps to help prevent a repeat occurrence.

Legal framework

This policy has due regard to statutory legislation and regulations including, but not limited to, the following:

- The Data Protection Act 1998
- The Computer Misuse Act 1990
- The General Data Protection Regulation (GDPR)

The policy also has due regard to the school's policies and procedures including, but not limited to, the following:

- E-Safety Policy
- Data Protection Policy
- Acceptable Use Policy

Types of security breach and causes

1. **Unauthorised use without damage to data** – involves unauthorised persons accessing data on the school system, e.g. 'hackers', who may read the data or copy it, but who do not actually damage the data in terms of altering or deleting it.
2. **Unauthorised removal of data –** involves an authorised person accessing data, who removes the data to pass it on to another person who is not authorised to view it, e.g. a staff member with authorised access who passes the data on to a friend without

authorised access – this is also known as data theft. The data may be forwarded or deleted altogether.

3. **Damage to physical systems** – involves damage to the hardware in the school's ICT system, which may result in data being inaccessible to the school and/or becoming accessible to unauthorised persons.
4. **Unauthorised damage to data** – involves an unauthorised person causing damage to data, either by altering or deleting it. Data may also be damaged by a virus attack, rather than a specific individual.

Breaches in security may be caused as a result of actions by individuals, which may be accidental, malicious or the result of negligence – these can include:

- Accidental breaches, e.g. as a result of insufficient training for staff, so they are unaware of the procedures to follow.
- Malicious breaches, e.g. as a result of a hacker wishing to cause damage to the school through accessing and altering, sharing or removing data.
- Negligence, e.g. as a result of an employee that is aware of school policies and procedures, but disregards these.

Breaches in security may also be caused as a result of system issues, which could involve incorrect installation, configuration problems or an operational error – these can include:

- Incorrect installation of anti-virus software and/or use of software which is not the most up-to-date version, meaning the school software is more vulnerable to a virus
- Incorrect firewall settings are applied, e.g. access to the school network, meaning individuals other than those required could access the system
- Confusion between backup copies of data, meaning the most recent data could be overwritten
- Mechanical failure, meaning that data could be lost or overwritten.

Secure configuration

An inventory will be kept of all IT hardware and software currently in use at the school, including mobile phones and other personal devices provided by the school. This will be audited on an annual basis to ensure it is up-to-date.

All systems will be audited on a termly basis to ensure the software is up-to-date. Any new versions of software or new security patches will be added to systems, ensuring that they do not affect network security, and will be recorded on the inventory.

Where practical, software that is out-of-date or reaches its 'end of life' should be removed from systems, i.e. when suppliers end their support for outdated products such that any security issues will not be rectified.

Network security

The school will employ firewalls in order to prevent unauthorised access to the systems.

The school’s firewall will be deployed as a:

- **Localised deployment**: the broadband service connects to a firewall that is located on an appliance or system on the school premises, as either discrete technology or a component of another system.

The Network Manager will ensure that:

- The firewall is checked weekly for any changes and/or updates
- Any changes and/or updates that are added to servers, including access to new services and applications, are checked to ensure that they do not compromise the overall network security.
- The firewall is checked weekly to ensure that a high level of security is maintained and there is effective protection from external threats.
- Any compromise of security through the firewall is recorded using the data breach log and is reported to the headteacher.

Malware prevention

The school understands that malware can be damaging for network security and may enter the network through a variety of means, such as email attachments, social media, malicious websites or removable media controls.

All school devices have secure malware protection and undergo regular malware scans.

The Network Manager will review and where necessary update malware protection on a termly basis to ensure it is up-to-date and can react to changing threats.

Malware protection will also be updated in the event of any attacks to the school’s hardware and software.

Filtering of websites will ensure that access to websites with known malware is blocked.

The school will use mail security technology, which will detect and block any malware that is transmitted by email. This will also detect any spam or other messages which are designed to exploit users.

User privileges

The school understands that controlling what users have access to is important for promoting network security. User privileges will be differentiated, i.e. pupils will have different access to data and the network than members of staff.

The Headteacher will be responsible for deciding what users have access to.

The Network Manager will ensure that user accounts are set up to allow users access to the facilities required, in line with the headteacher's instructions, whilst minimising the potential for deliberate or accidental attacks on the network. use upper and lowercase letters, as well as numbers, to ensure that passwords are strong. Users will also be required to change their pass

Users will be required to change their passwords every 90 days and will be required to follow password protocols as set by the school.

Pupils are responsible for remembering their passwords; however, staff and the IT Team will be able to reset them if necessary.

An individual user account will be created for visitors to the school, such as volunteers, and access will be filtered as per the school settings. Access will not be granted for any period longer than the visitor is in school.

Monitoring usage

Monitoring user activity is important for the early detection of attacks and incidents, as well as inappropriate usage by pupils or staff.

Pupils and staff are aware that that their usage will be monitored, in accordance with the school's Acceptable Use Policy and E-Safety Policy.

If a user accesses inappropriate content or a threat is detected, an alert will be sent to the Assistance Headteacher with responsibility for IT or the School Business Manager who will investigate, record and take appropriate remedial action.

Removable media controls and home working

The school understands that pupils and staff may need to access the school network from areas other than on the premises. Effective security management, via two step verification and encryption, will be established to prevent access to, or leakage of, data, as well as any possible risk of malware.

Staff laptops and any other device which staff have been authorised to take off site will be encrypted. The use of un-encrypted USB's and hard drives has been prohibited to prevent unauthorised access to personal data should they be lost or misplaced.

Pupils and staff are permitted to use registered personal devices.

The Wi-Fi networks at the school will be restricted and password protected. Access to wifi will be controlled by the Network Manager.

Separate Wi-Fi networks will be established for students and visitors to the school to limit their access to applications which are not necessary.

Backing-up data

A backup of all electronic data is taken daily.

An incremental backup of any data that has changed since the previous backup will be taken daily.

Where possible, back-ups are run overnight and are completed before the beginning of the next school day.

Upon completion of back-ups, data is stored on the school’s hardware which is password protected.

Data is also replicated and stored in Google Drive.

Only authorised personnel are able to access the school’s back up data. This is usually the Network Manager, the IT team the Headteacher and delegated members of the Senior Leadership Team.

Security Breach Incidents

Any individual that discovers a security data breach will report this immediately to the Headteacher or Business Manager.

Security breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

When an incident is raised, the **Headteacher or Business Manager** will record the following information:

- Name of the individual who has raised the incident
- Description of the incident
- Description of the data which may be compromised
- Description of any perceived impact
- Description of any devices involved, e.g. school-owned laptop
- Location of the equipment involved
- Contact details for the individual who discovered the incident

The Headteacher's representative (usually a member of SLT) will take the lead in investigating the security breach, and will be allocated the appropriate time and resources to conduct this.

As quickly as reasonably possible, they will ascertain the severity of the breach and determine if any personal data is involved or compromised.

If there has been a breach of personal data then the Data Breach Procedure must be followed.

Remedial Action

Where the security risk is high, the school will establish what steps need to be taken to prevent further data loss which will require support from various school departments and staff. This action will include:

- Informing relevant staff of their roles and responsibilities in areas of the containment process
- Taking systems offline
- Retrieving any lost, stolen or otherwise unaccounted for data
- Restricting access to systems entirely or to a small group
- Backing up all existing data and storing it in a safe location
- Reviewing basic security, including:
  - Changing passwords and login details on electronic equipment.
  - Ensuring access to places where electronic or hard data is kept is monitored and requires authorisation.

Where appropriate, e.g. if offences have been committed under the Computer Misuse Act 1990, the Headteacher will inform the police of the data breach.

Consideration of further notification

The school will consider whether there are any legal, contractual or regulatory requirements to notify individuals or organisations that may be affected or who will have an interest in security.

The school will assess whether notification could help the individual(s) affected, and whether individuals could act on the information provided to mitigate risks, e.g. by cancelling a credit card or changing a password.

If a large number of people are affected, or there are very serious consequences, the ICO will be informed.

The school will consider who to notify, what to tell them and how they will communicate the message, which may include:

- A description of how and when the security breach occurred and what data was involved. Details of what has already been done to respond to the risks posed by the breach will be included.
- Specific and clear advice on the steps they can take to protect themselves, and what the school is willing to do to help them.
- A way in which they can contact the school for further information or to ask questions about what has occurred.

The school will consult the ICO for guidance on when and how to notify them about security breaches.

The school will consider, as necessary, the need to notify any third parties – police, insurers, professional bodies, funders, trade unions, website/system owners, banks/credit card companies – who can assist in helping or mitigating the impact on individuals.

Under the GDPR, the following steps will be taken if a breach of personal data occurs:

The school will implement its Data Breach Procedure and will notify the ICO within 72 hours of a breach where it is likely to result in a risk to the rights and freedoms of individuals.

Where a breach is likely to result in significant risk to the rights and freedoms of individuals, the school will notify those concerned directly with the breach.

Evaluation and response

The school will identify any weak points in:

- Existing security measures and procedures
- Levels of security awareness and training.

And with the approval of the school leadership team, implement the recommendations of the report after analysis and discussion.

Monitoring and review

This policy will be reviewed by the Headteacher in conjunction with the Senior Leadership Team on an **annual** basis.

The effectiveness of this policy will be monitored and will be amended as necessary with any changes communicated to staff members.

Issue Date May 2018
Last review date January 2020