The Castle Partnership Trust

ACHIEVE | BELONG | PARTICIPATE

The Castle School

ACHIEVE | BELONG | PARTICIPATE

Information Security Policy

Date: June 2018

Executive Headteacher: Sarah Watson
Acting Headteacher Court Fields School: Polly Matthews
Headteacher Wellesley Park School: Carly Wilkins
Head of School The Castle School: Fran Gormley

Due for review: Summer Term 2021

Lead Person: Business Manager

1. Introduction

The Trust's investment in the acquisition, storage and use of electronic and paper based information exists primarily to help provide the effective delivery of its services. This information is held about a variety of people and it is essential that the availability, **integrity,** and confidentiality of accurate relevant information is maintained in a secure and legal environment.

2. Objective

The information security objective is to ensure that the Trust's information bases are protected against identified risks so that it may continue to deliver its services and obligations to the community. It also seeks to ensure that any security incidents have a minimal effect on its business and academic operations.

3. Policy

The purpose of this policy is to protect the Trust's information assets from all threats, whether internal or external, deliberate or accidental.

The key aims of the policy are to ensure that:

- Information is protected from unauthorised access
- Confidentiality of personal or sensitive information is assured
- Integrity of information is maintained
- Information is disposed of in a timely, appropriate and secure manner
- Legislative requirements **(mainly deriving from the Data protection Act 1998 and the General Data Protection Regulation [GDPR])** and Trust policies and practices are observed
- Information security training is available to all relevant staff
- Appropriate monitoring and reporting processes are put in place to identify and act upon breaches of information security

The policy applies to all form of information, including, but not restricted to, text, pictures, photographs, maps, diagrams, video, audio, CCTV and music, which is owned by the school including information which is:

- **Spoken face to face, by mobile telephone or written on paper or printed out from a computer system. This may include working both onsite or remotely (e.g. at home)**
- **Transmitted by electronic mail, over the Internet and via wireless technology**

- **Stored and processed via computers, computer networks or mobile computing devices, including, but not restricted to, PCs, mobile phones, laptops, tablet PCs, electronic organisers or stored on any type of removable computer media**

4. Supporting Framework

In order to achieve this, the Trust will develop and maintain information security standards. These will be based on, but will not necessarily correspond in depth with, the British Standard on Information Security.

Procedures, working practices and protocols will be developed as required by educational or organisational needs. Examples of measures to achieve the above are physical security, virus control and the use of passwords for access control. The development of any new system will include information security analysis and requirements as part of the initial specification.

5. Responsibilities

The Headteacher of each school, has direct responsibility for maintaining this policy and providing advice and guidance on its implementation.

All staff are responsible for policy implementation and for ensuring that their staff adhere to the standards. **The policy applies wherever and whenever school information is processed.**

6. Implementation

This policy will be made available to all parents, guardians, staff (whether permanent or temporary) and governors.

7. General Security

It is important that unauthorised people are not permitted access to school information and that we protect against theft of both equipment and information. This means that we must pay attention to protecting our buildings against unauthorised access **and also adopt the following practices: .**

- Do not reveal pin numbers or building entry codes to people that you do not know or who cannot prove themselves to be employees.
- If you don't know who someone is and they are not wearing some form of identification, ask them why they are in the building.
- Do not position screens on reception desks where they could be seen by members of the public
- Do not be afraid to challenge people who you do not recognise if they are not wearing an identity badge
- Lock secure areas when you are not in the office
- Beware of people tailgating you into the building or through a security door

- Do not let anyone remove equipment or records unless you are certain who they are.

Visitors and contractors in school buildings should always sign in and out using a visitors' book.

8. Security of Paper Records

Paper documents should always be filed correctly**. and trust employees will be asked to adhere to the following procedures:**

- Records that contain personal data, particularly if the information is sensitive**,** should be locked away when not in use and should not be left open or on desks overnight or when you are not in the office.
- Always keep track of files and who has them
- Do not leave files out where others may find them.
- Where a file contains confidential or sensitive information, do not give it to someone else to look after.

Paper records should be disposed of with care. If papers contain confidential or sensitive information shred them before disposing of them or ensure they are placed in one of the sacks/bins provided by the school's confidential waste contractor. Particular care must be taken when selecting papers to be placed in a recycling bin.

9. Electronic software

Trust employees will be expected to adhere to the following procedures:

- Prevent access to unauthorised people and to those who don't know how to use an item of software properly. It could result in loss of information.
- Keep suppliers CDs containing software safe and locked away. Always label the CDs so you do not lose them in case they need to be re-loaded.
- When we buy a license for software, it usually only covers a certain number of machines. Make sure that you do not exceed this number as you will be breaking the terms of the contract.

Guidance for your password is:

- Don't write it down
- Don't give anyone your password.
- Your password should be at least 6 characters
- Your password should be something that you can remember but not anything obvious (such as *password*) or anything that people could guess easily such as your name.
- You can be held responsible for any malicious acts by anyone to whom you have given your password.
- Try to include numbers as well as letters in the password
- Take care that no-one can see you type in your password

- Change your password regularly, and certainly when prompted. Also change it if you think that someone may know what it is.

Many database systems, particularly those containing personal data should only allow a level of access appropriate to each staff member. The level may change over time.

- Lock your computer and laptop by using CTRL/ ALT/ DEL when you are away from it for any length of time. Mobile devices should also be locked.

10. Use of E Mail and Internet

- To avoid a computer virus arriving over the Internet, do not open any flashing boxes or visit personal websites.
- **Encrypt** highly confidential or sensitive personal information **being sent via** e mail
- Save important e mails straight away.
- Unimportant e-mails should be deleted straight away.
- Do not send information by e mail which breaches the Data Protection Act **or the GDPR**. Do not write anything in an e mail which could be considered inaccurate or offensive, and **which** cannot be substantiated.

11. Electronic Hardware

Trust employees will be expected to adhere to the following procedures:

- All hardware held within each School should be included on the relevant asset register.
- The register should be kept up to date at all times.
- Do not let anyone remove equipment unless you are sure that they are authorised to do so
- In non-secure areas, consider using clamps or other security devices to secure laptops and other portable equipment to desk tops.

Disposing of hardware.

Computers to be disposed of must be completely 'cleaned' before disposal. It is not enough just to delete all the files.

12. Home working guidance

Trust employees will be expected to adhere to the following procedures:

In essence, if you work outside the school or at home, the guidance is the same as given above, However, you may need to consider these extra points. Information is more liable to be lost or stolen outside the office:

- Do not access confidential information when you are in a public place (such as a train) and may be overlooked.

- Do not have conversations about personal or confidential information when in a public place. Ensure that, if urgent, you have your conversation in a separate room or away from other people.

If you use a laptop or mobile device:

- Ensure that it is locked and password protected to prevent unauthorised access.
- Make sure that you don't leave your laptop or mobile device anywhere it could be stolen. Keep it with you at all times and secure it when you are in the school.
- When working on confidential documents at home do not leave them lying around where others may see them; dispose of documents using a shredder.
- If confidential information is taken in electronic format it must be password protected or stored on an encrypted memory stick.
- If you are using your own computer, ensure that documents cannot be accessed by others. When you have completed working on them, transfer them back to the school and delete them from your computer.

Glossary of legislation

The Data Protection Act 1998

The General Data Protection Regulation (GDPR)

The Freedom of Information Act 2000

The Environmental Information Regulations 1992

The Human Rights Act 1998

The Regulation of Investigatory Powers Act

Copyright and Intellectual Property rights

The Computer Misuse Act