Data Security Policy

Purpose

The purpose of this policy is to help protect our school against information vulnerabilities and prevent unauthorised access, loss or disclosure as per the GDPR regulations.

Scope

This policy applies to anyone who is accessing the schools information, systems and buildings

Governance

- We will identify someone who will have overall accountability for managing information risks;
- We will ensure our school has a database of information assets and staff accountable for those assets;
- We will ensure our school has a recognised process for identifying and investigating information incidents and breaches - please see incident handling procedure;
- We will ensure information is kept up-to-date and accurate at all times;
- We will ensure information is safely and securely disposed of after it reaches its retention period
- We will have plans in place to ensure the continuity of our school business in the event of an unforeseen incident occurring;

Technical Security

- We will ensure all electronic devices and removable media are encrypted;
- We will ensure staff password protect all electronic devices and never share them;
- We will ensure passwords are changed regularly;

- We will ensure electronic devices and removable media are wiped cleaned and disposed of securely at the end of their use;
- We will make regular back-ups of our data on electronic devices and systems;
- We will protect the schools electronic devices and systems against viruses, malware, malicious codes and cyber-attacks by installing the latest security software;

Remote Working

- If staff working are away from the office, they will only take the minimum physical information required;
- If staff are transporting physical information, they will ensure it is kept out of sight and secure;
- If staff are working from home, they will ensure the schools information is kept private from family members and ensure there is a secure authentication process;

Staff

- We will ensure information is removed and secured from staff leaving employment of the organisation;
- We will consider existing and future access and permission controls for staff, i.e. is it still appropriate for them to have access to the same information if they change positions;
- We will ensure we are satisfied and assured about the people who are working for our school before giving them access to our information e.g. references, vetting, clauses in contracts etc.;

Physical Security

- We will ensure physical information is always stored in either locked filing cabinets and/or locked offices;
- We will ensure our school has a clear desk procedure and staff adhere to it;
- We will ensure staff lock the screen of their PC whenever they are away from their desk;

- We will ensure access to non-public accessible areas in buildings is controlled;
- All visitors sign in when arriving and out when leaving
- All visitors are escorted through the building by a member of staff
- Appropriate access locks are fitted to areas of the building containing sensitive information
- Ensure all staff are wearing identification badges
- When vacating or moving offices, we will undertake a thorough sweep of the building to ensure all information has been removed – check left over furniture, basements, lofts etc.;
- We will ensure paper records are disposed of securely using a cross-cutting shredder or a reputable confidential waste company;

Additional information

- We will ensure that our school:
- Undertakes regular training of staff, including during induction, to ensure they understand their responsibilities under the above headings;
- Provides information so that staff understand and recognise an information security incident and know what to do;
- Conducts regular monitoring to ensure the policy headings above are in place and adhered to;
- Keeps apace with recommended industry standards on the IT estate for both hardware and software wherever possible;
- Provides regular communications to staff about what to look for in respect of cyber-attacks;
- Makes all contractors, agency staff and temporary staff are aware of their responsibilities under this policy.

Policy Ratified on 22/03/2018 by the Full Governing Board

Glossary

Information assets A body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited. Information assets have value, risk, content and lifecycles

Incidents A suspected, attempted, successful, or imminent threat of unauthorized access, use, disclosure, breach, modification, or destruction of information; interference with information technology operations; or significant violation of responsible use policy

Breaches A data breach is the intentional or unintentional release of secure or private/confidential information

Electronic devices Includes computers, mobile phones, tablets and pads

Removable media Any type of storage device that can be removed from a computer while the system is running. Include CDs, DVDs and Blu-Ray disks, as well as diskettes and USB drives. Removable media makes it easy for a user to move data from one computer to another

Encrypted Encryption is the conversion of electronic data into another form, which cannot be easily understood by anyone except authorized parties. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it

Viruses A computer virus is a program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes. Viruses can also replicate themselves

Malware Short for malicious software, malware refers to software programs designed to damage or do other unwanted actions on a computer system

Malicious code Any code in any part of a software system or script that is intended to cause undesired effects, security breaches or damage to a system

Cyber-attacks A deliberate exploitation of computer systems, technology-dependent enterprises and networks. Cyberattacks use malicious code to alter computer code, logic or data, resulting in disruptive consequences that can compromise data and lead to cybercrimes, such as information and identity theft

Physical information Includes paper records and files

Hardware The physical aspect of computers, telecommunications, and other devices

Software The various kinds of programs used to operate computers and related devices