SUMMARY GUIDANCE – SCHOOLS INFORMATION SECURITY POLICY

'Information security is everyone's responsibility'

This is a summary of the Schools Information Security Policy (SISP). A full version of the document can be found in the staff handbook.

1. Why do we need security?

Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post, email, and even spoken in conversations.

The purpose of information security is to ensure that all information (including personal information) and associated processing systems are protected to an adequate level from events that may cause personal distress or have a negative impact on the School and its services.

This policy promotes good practices in respect to information security ensuring 3 main principles are embedded in the authorities' manual/electronic records management systems:

Confidentiality	Integrity	Availability
Information only accessed by authorised individuals	Safeguards accuracy and completeness of information	Ensure authorised officers have access when needed

Information security is not all about protecting the School from financial penalties it is about respecting the lives and rights of the residents/partners in our community and our employees.

2. Lost Information

You should always report any instances of lost personal information or where it has been sent to the wrong person(s) immediately to the Head Teacher so the risks and impacts can be properly managed. Do not forget information security concerns many things including letters, reports, emails, paper files, etc, but can also include issues such as lost laptops, work mobile phones, lost digital cameras, lost memory sticks, etc. See the Information Security Breach Procedure (ISBP) in the staff handbook.

3. Sharing Information

What should a School officer consider when asked to share personal identifiable information (PII) with other third parties?

- Only share PII if you have the legal justification to do so
- Share information in compliance with the SISP and Information Sharing Policy
- Know the objective/reasons for sharing PII
- Investigate whether the objective can be met another way without sharing PII
- Send elements of PII that are definitely required to meet the objective/reasons
- Where possible, anonymise the information you send so it is not personally identifiable
- Confirm the recipients contact details before sharing information
- Appropriately protect the PII you are sharing by either using encryption / password if it is electronic, by using special delivery if posting, etc.

4. Sensitive Information

The School handles numerous types of sensitive data on a day-to-day basis. The following are a list of do's and don'ts in respect to handling sensitive data.

Do's	Don'ts
If you lose any sensitive or personal information then this should be reported immediately to your Head Teacher	Do not store sensitive or personal information on portable media (laptops, memory sticks, CD's, etc) unless in very exceptional circumstances and when the media is encrypted
When discussing sensitive or personal information on the phone consider who may be listening in at both ends of the phone line	Do not give out sensitive information unless the person is authorised to receive it and the data owner has approved that you can send it
Understand your responsibilities under the UK Data Protection Act 2018 and full version of the School Information Security Policy (SISP).	Do not leave sensitive or personal information on printers, computer screens or desks whilst away from your desk
Keep sensitive information stored securely and restrict access on a need to access basis	Do not access any sensitive or personal information that is not relevant to your role
Ensure that sensitive data, both paper based and electronic are shredded / disposed of correctly	

5. Passwords

It is your responsibility as a user to:

- Do not share passwords
- If you think someone is aware of your password change it straight away
- Avoid writing down passwords
- Make passwords hard to guess; try to avoid using family names.
- Ensure your password includes upper and lower case letters, numbers and a special character (not a number or letter, e.g. an exclamation mark)
- Change your password every 3 months or when prompted to do so.

6. Email/Other Communication Technologies (OCT)

See full copy of SISP for what is defined as reasonable use of email/OCT. Appropriate use includes:

- Email/OCT (private on School equipment) must not contain indecent, inappropriate or offensive content
- Take care when addressing email messages to ensure a correct address is used
- Do not send personal or sensitive information via unprotected email
- Reasonable personal use is allowed in non-work time only
- Do not take part in chain letter emails

7. Internet

You should always remember that your School internet access is primarily provided for business use. See full copy of SISP for what is defined as reasonable use of the internet. Please note:

- All internet use on School equipment is logged for management purposes
- Reasonable personal use is permitted in non-work time
- Do not use the School's internet (both within and outside working hours) to access inappropriate, offensive, illegal or adult/sexually explicit material. A full list of types of website that are unauthorised is detailed in the full version of the SISP
- Do not leave the internet logged on when you leave your computer unattended

8. SISP – Summary of Key Messages to Employees

YOU MUST:

- Ensure you take steps to safeguard the security of information you hold/access
- Comply with the SISP, associated acceptable use policies and the information breach procedure
- If you handle personal information, have an adequate awareness of your UK Data Protection Act/GDPR responsibilities
- Report lost/stolen ICT equipment/personal information to your Head Teacher
- Complete information governance training
- Only share personal information if there is legal justification to do so
- Where possible anonymise personal information shared with non-School parties, e.g. use a reference number and not a name
- Appropriately protect information that is being shared
- Confirm the recipients details, e.g. email address, location, etc. before sharing the information
- Only access information/systems that you need to undertake your duties
- Use secure passwords and never share them with your colleagues
- Direct external parties that need access to the School's network to the ICT Technician
- Lock down your pc/laptop when you leave it unattended for a prolonged period
- Be responsible for the physical security of School ICT equipment and information in your possession (i.e. paper files) making sure that these are securely stored
- Ensure your mobile device has PIN security activated
- Only use USB sticks or other removable media (e.g. external hard drives, digital cameras, etc) on an exception basis and only use those that are encrypted
- Ensure information held on removable media is encrypted/password protected
- If you are mobile/home worker, ensure that ICT equipment and information used on the road or at home, is locked down/away securely when not in use
- Never leave ICT equipment and/or personal information in a car overnight
- Do not use email on School equipment/networks for personal use in works time
- Only use the internet for personal use in non-work time
- Undertake a data protection impact assessment on all new/developed ICT systems that involve processing/viewing of personal information