Windmill Hill Primary School

Data Security Policy

The accessing and appropriate use of school data is something that the school takes very seriously.

The school follows the Local Authority guidance documents listed below

- Appendix A –
  Headteacher's Guidance – Data Security in Schools – Dos and Don'ts

- Appendix B
  Network Manager/MIS Administrator or Manager Guidance – Data Security in Schools

- Appendix C
  Staff Guidance – Data Security in Schools – Dos and Don'ts

- Appendix D
  SIRO/IAO Guidance – Data Security in Schools - Dos and Don'ts

The Headteacher, SIRO and Network Manager documents contain advice about identifying information assets including an example of an excel spreadsheet and a brief outline of the school policy that can be displayed at appropriate sites within the school or handed to visitors or guests.

Security

- The School gives relevant staff access to its Management Information System, with a unique ID and password

- It is the responsibility of everyone to keep passwords secure

- Staff are aware of their responsibility when accessing school data

- Staff have been issued with the relevant guidance documents and the Policy for ICT Acceptable Use

- Staff have read the relevant guidance documents available on the Council's Intranet – Becta' s "Good practice in information handling: Keeping data secure, safe and legal".

  This document is available on the Council's Intranet – Resources/ICT Services/Information Guidance for Schools// Information Security.

- Leadership team has identified Senior Information Risk Owner (SIRO) and Asset Information Owner(s) (AIO) as defined in the guidance documents detailed above.

- Staff members keep all school related data secure. This includes all personal, sensitive, confidential or classified data

- staff must not leave any portable or mobile ICT equipment or removable storage media in unattended

- It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents faxed, copied, scanned or printed. This is particularly important when shared copiers (multi-function print, fax, scan and copiers) are used

- Anyone expecting a confidential/sensitive fax should have warned the sender to notify before it is sent.

Impact Levels and Protective Marking

- Appropriate labelling of data should help schools secure data and so reduce the risk of security incidents
- Apply labelling in accordance with guidance from your Senior Information Risk Owner (SIRO)
- Most learner or staff personal data will be classed as Protect
- Protect and caveat classifications that schools may use are;
  - PROTECT – PERSONAL e.g. personal information about an individual
  - PROTECT – APPOINTMENTS e.g. to be used for information about visits from the Queen or government ministers
  - PROTECT – LOCSEN e.g. for local sensitive information
  - PROTECT – STAFF e.g. Organisational staff only
  - RESTRICTED – STAFF e.g. A large amount of data (information on over 20 persons)
  - RESTRICTED – PUPILS e.g. A large amount of data (information on 20 persons)
- Applying too high a protective marking can inhibit access, lead to unnecessary and expensive protective controls, and impair the efficiency of an organisation's business
- Applying too low a protective marking may lead to damaging consequences and compromise of the asset
- The sensitivity of an asset may change over time and it may be necessary to reclassify assets. If a document is being de-classified or the marking changed, the file should also be changed to reflect the highest marking within its contents

Reviews are continuing to look at the practical issues involved in applying protective markings to electronic and paper records and government representatives are working with suppliers to find ways of automatically marking reports and printouts.

Senior Information Risk Owner (SIRO)

The SIRO is a senior member of staff who is familiar with information risks and the school's response. Typically, the SIRO should be a member of the senior leadership team and have the following responsibilities:

- they own the information risk policy and risk assessment
- they appoint the Information Asset Owner(s) (IAOs)
- they act as an advocate for information risk management
- The Office of Public Sector Information has produced "Managing Information Risk".

  This document is available on the Council's Intranet – Resources/ICT Services/Information Guidance for Schools// Information Security.

- The SIRO in this school is Paula Newman

Information Asset Owner (IAO)

Any information that is sensitive needs to be protected. This will include the personal data of learners and staff; such as assessment records, medical information and special educational needs data. Please refer to the appendix at the back of this document showing examples of information assets a school may hold. Schools should identify an Information Asset Owner. For example, the school's Management Information System (MIS) should be identified as an asset and should have an Information Asset Owner. In this example the MIS Administrator or Manager could be the IAO.

The role of an IAO is to understand:

- what information is held, and for what purposes
- what information needs to be protected (e.g. any data that can be linked to an individual, pupil or staff etc including UPN, teacher DfE number etc)
- how information will be amended or added to over time
- who has access to the data and why
- how information is retained and disposed off
- The IAO in this school is Gill Gleave.

As a result, the IAO is able to manage and address risks to the information and make sure that information handling complies with legal requirements. In a Secondary School, there may be several IAOs, whose roles may currently be those of e-safety coordinator, ICT manager or Management Information Systems administrator or manager.

Although these roles have been explicitly identified, the handling of secured data is everyone's responsibility – whether they are an employee, consultant, software provider or managed service provider. Failing to apply appropriate controls to secure data could amount to gross misconduct or even legal action.