Information Security Policy

OLDFIELDS HALL MIDDLE SCHOOL

2020

Approved by Governing Body on

21.11.20

Date of next scheduled revision

November 2021

Contents

1. Introduction

1.1 Information Security

The availability of complete and accurate information is key to providing excellent services to the pupils, parents and staff of Staffordshire schools. Staffordshire schools hold and process a large amount of confidential and personal information on private individuals, employees, service partners, suppliers and its own operation.

Leicestershire schools have a number of responsibilities to protect their reputation as well as safeguarding individuals from the possibility of information and systems misuse or infringement of personal privacy. Therefore the **confidentiality**, **integrity**, **availability** and **accountability** of this information need to be protected from harm in a way that is proportionate to the risks to the information.

This Information Security Policy provides the overall framework to help everyone play his or her part in protecting pupil and staff information. It is consistent with Staffordshire County Council's corporate strategies on ICT and information management. This constitutes the high level policy.

This policy is supported by a comprehensive set of detailed policies, processes, procedures and guidelines, which constitute the Information Security Management Framework (ISMF).

A glossary of information security terms used in this policy is provided in Appendix A.

1.2 Scope

The Information Security Policy applies to everyone who reads or processes school information. The policy applies **wherever** and **whenever** school information is processed and applies equally to **all users** including:

- Teachers, Governors, Teaching Assistants, Auxiliary Staff and Office Staff
- Contractors, consultants, casual and temporary employees and volunteers
- Partners and suppliers

Please note that throughout this document, the words "employee" and "user" are used to cover all the groups of people listed above.

The Information Security Policy applies to **all forms of information**, including, but not restricted to, text, pictures, photographs, maps, diagrams, video, audio, CCTV and music, which is owned by, administered or controlled by the School, including information, which is:

- Spoken face to face, communicated by fixed line, by mobile telephone, or by two-way radio
- Written on paper or printed out from a computer system. This may include working both on-site or remotely (e.g. at home)
- Stored in structured manual filing systems (see Appendix A, Glossary of Terms)
- Transmitted by electronic mail, fax, over the Internet and via wireless technology

- Stored and processed via computers, computer networks or mobile computing de
- Devices, including, but not restricted to, PCs, mobile phones, laptops, tablet PCs, electronic organisers and personal digital assistants (PDAs).
- Stored on **any** type of removable computer media including, but not restricted to CDs, DVDs, tapes, microfiche, diskettes, USB memory sticks, external hard disks, and memory stores in devices including, but not restricted to, digital cameras, MP3 and MP4 players.

1.3 Purpose

The purpose of the Information Security Policy is:

- To protect the School's Information and subsequently to protect the School's reputation
- To enable secure information sharing to deliver services
- To protect the School from legal liability and inappropriate use
- To encourage consistent and professional use of information and systems
- To ensure everyone is clear about their roles in using and protecting information
- To maintain awareness of information security
- To protect the School's employees
- NOT to constrain reasonable use of information in support of normal business activities of the School

This policy shall be seen as additional to all other school policies relating to information disclosure and personal conduct.

1.4 Breaches of the Information Security Policy

Actions or neglect leading to a breach of this policy will be investigated, which could result in disciplinary action; this could include dismissal without notice even for a first offence if sufficiently serious.

Breaches of this policy by a user who is not a direct employee of the School may result in action being taken against the user and/or their employer.

In certain circumstances the matter will be referred to the police to consider whether criminal proceedings should be instigated.

Breaches of the Data Protection Act 2018 could result in a hefty fine being issued to the individual and the organisation.

1.5 Legal Framework for Information Security

Line managers and individuals have responsibilities regarding the legal use of information. There are many laws and legal rules governing how information is handled. The list below demonstrates the importance of using information correctly.

- Common law in relation to duties of confidentiality
- Health and Safety at Work Act 1974
- Theft Act 1978
- Indecent display (Control) Act 1981
- Obscene Publications Act 1984
- Regulation of Investigatory Powers Act 2000
- Data Protection Act 2018
- Human Rights Act 1998
- Protection of Children Act 1999
- Freedom of Information Act 2000

- Copyright, Designs and Patents Act 1988
- Computer Misuse Act 1990

This list is not exhaustive and will change over time. Users shall seek guidance about the legal constraints of using information in their work and the School, through the Council will provide appropriate guidance and training to its staff if requested.

1.6 Further Information about Information Security

Further information can be found by contacting Mr C Gliddon (Headteacher)
Information

2. Information Security Roles and Responsibilities

2.1 All information users including all employees, contractors, consultants, volunteers, governors, partners and suppliers must:

1. **Comply with** this Information Security Policy, processes, procedures and guidelines at all times.
2. Comply with legal, statutory, regulatory and contractual obligations related to information at all times.
3. Be familiar with the operation and security requirements of the information and computer systems, to minimise the possibility of harm to **confidentiality**, **integrity** and **availability**.
4. Observe the utmost care when dealing with personal and sensitive information to ensure that it is never disclosed to anyone inside or outside the School without proper authorisation.
5. Report immediately all suspected violations of this and all other security policies, system intrusions, and any other security incidents or weaknesses in security, which might jeopardise the School's information or information systems, following agreed incident management policies and processes. Appendix B of this document sets out who suspected violations should be reported to. Where an individual feels that he/she is unable to report the issue to the head of establishment, he/she is reminded of the existence of the LA's Whistleblowing Policy, a copy of which is accessible in the School, which sets out additional avenues to report concerns, outside of the establishment itself
6. Read and act on any communications and training about information security and ask for clarification if these are not understood.
7. Play an active role in protecting information in day-to-day work.

2.2 Governors and School Senior Leadership Team

1. Approve this high level Information Security Policy.
2. Actively promote effective and appropriate information security by the use of structured risk assessment in all future developments and by appropriate retrospective risk assessment of current processes and systems.
3. Implement and promote Information Security to all staff within their service areas.
4. Ensure that employees understand and abide by the Information Security Policy and its associated policies, processes, procedures, guidelines and understand its impact
5. Assign owners to all information in their area of responsibility
6. Provide effective means by which all staff can report security incidents and weaknesses, and act on all such reports according to agreed incident management policies and processes.
7. Apply security controls relating to Human Resources and ensure that job descriptions address all relevant security responsibilities.
8. Provide written authorisation for access to information.
9. Ensure that communications regarding information security are cascaded effectively to all staff.
10. Ensure that information security is an integral part of all departmental processes.

2.3 Information owners

Data sets may have different owners and where several potential information owners exist, responsibility should be assigned to the manager whose group makes the greatest use of the data. For example, Office Managers, Bursars

1. Use structured risk assessment to select security controls to protect their information.
2. Monitor to ensure security controls continue to be effective and that information is being handled correctly.
3. Report and act on security incidents and weaknesses relating to their information according to agreed incident management policies and processes.
4. Manage the residual risks to their information.
5. Prepare appropriate Business Continuity plans and contingency arrangements.

2.4 ICT Services

1. Be the custodian of electronic information in its care by implementing and administering technical security controls as specified in the information security policies, and by the Information Owners as a result of information security risk assessment.
2. Assist Information Owners in identifying technical information security risks and appropriate technical security controls.
3. Assist schools to ensure all software is licensed and remove unlicensed software
4. Provide contingency arrangements for information systems
5. Provide appropriate protection from malicious software.
6. Monitor and report breaches of this policy including unauthorised attempts to access information or systems.
7. Monitor and investigate technical security breaches.
8. Provide technical support to enable compliance with this policy.

3. Information Security Policy

3.1 The School operates within the law at all times	1. Information shall be used **legally** at all times, complying with UK and European law. All users, including employees, and agents of the School might be held personally responsible for any breach of the law. 2. All personal information processed electronically or held in a structured manual filing system shall be processed in accordance with the **Data Protection Act 2018**. Utmost care shall be taken when dealing with personal and sensitive information to ensure that it is never disclosed to anyone inside or outside the School without proper authorisation. 3. Advice shall be sought from Data Protection Officer about what information is covered by the Data Protection Act and for detailed guidance about how to handle such information. 4. Personal, confidential or sensitive information **shall be protected** appropriately at all times and in particular when removed from School premises either physically on paper or electronic storage devices, or when transmitted electronically outside the School. 5. Personal, confidential or sensitive information shall not be included in the text of e-mails to be sent outside the authority, or in files attached to them, unless these are securely encrypted or sent by secure network links. Please be confident that the link is secure before this is used. 6. Any request for information under the **Freedom of Information Act 2000** (FOIA) shall be handled in accordance with the law and processed within 20 working days. Anyone handling FOIA requests shall have completed the appropriate level of training. Where an exemption to FOIA might apply, further advice shall be obtained from Staffordshire Governance. 7. Information **shall not be used** in any way that might be seen as defamatory, libellous, insulting or offensive by others, Electronic and non-electronic communications shall not contain material that is profane, obscene, indecent, pornographic, defamatory, inflammatory, threatening, discriminatory, harassing (racially, sexually or otherwise offensive), subversive or violent, racist or of an extreme political nature, or which incites violence, hatred or any illegal activity. **Note;** It is accepted that in some professional situations such information is required for business reasons. 8. The School shall only use **licensed software** on its computers, servers and other computing devices such as personal digital assistants (PDAs). The School shall provide sufficient legally acquired software to meet all legitimate and agreed needs in a timely fashion. **9.** Information, including text, still and moving pictures, photographs, maps, diagrams, music and sound recording shall not be saved, processed or used in breach of **copyright**

3.2 Access to information shall be controlled	1. The requirements for **confidentiality**, **integrity**, **availability** and **accountability** shall be determined for all information, from creation to deletion. 2. Structured **information security risk assessment** shall be used to determine the appropriate security controls required to protect information, which are proportionate to the risks to the information and information systems. This risk assessment shall be done as part of system and process development. The effort expended on risk assessment and the amount of formal documentation required shall be proportionate to the perceived risks to the information and the impact of a breach of its security. 3. Access to information shall be **authorised** by management, including sharing information with partners and other organisations. Briefings and formal acceptance of security policies are required **before** access is granted to certain information systems and facilities. 4. There shall be adequate **separation** of functions for tasks that are susceptible to fraudulent or other unauthorised activity; Audit shall be consulted for advice on this. 5. Information users shall not attempt to access information to which they do not have **authority**. 6. Information users shall keep personal **passwords** confidential at all times. 7. **Agreements and contracts** with external business partners and suppliers shall include the requirement to adhere to this policy, where there is relevance to do so. 8. All **equipment**, including network equipment, attached to the School's computer network shall be approved by the Head Teacher **before** connection. 9. School equipment, facilities and information shall be used only for the School's **business purposes**, unless written permission of line management has been obtained. School equipment, facilities and information must never be used for personal gain or profit. 10. **Non-School** or **personally owned** equipment or storage devices shall not be connected to the School computer network or to any School-owned equipment, whether on the School's network or not, without written permission from the Head Teacher 11. All information about the **security arrangements** for School computer and network systems and structured manual filing systems is confidential to the School and shall not be released to people who are not authorised to receive that information.
3.3 The availability of information shall be protected	1. Business continuity plans shall include all aspects of the School's **infrastructure**, which are required to maintain the continuity of all critical business processes and support services. This shall include, but not be limited to, manual filing systems, information systems, information on mobile devices and storage, communications including telephone services, staffing requirements, transport facilities, electricity supply, office accommodation and maps.

3.4 The integrity of information shall be maintained	1. A named individual should have operational responsibility for the ICT systems and procedures (e.g. Network Manager). Details of key staff are listed at Appendix B of this policy. 2. The accuracy and completeness of information, including structured manual filing systems, processing methods and computer software shall be **protected** from unauthorised modifications. Users shall not attempt unauthorised modifications. 3. Users shall use only the **officially provided or approved facilities and systems** to access School information. 4. Users shall not interfere with the **configuration** of any computing device without approval 5. Update regularly all devices, which are subject to the threat of **malicious software**, with malicious software scanning software. 6. Update regularly all devices, which are subject to the threat of **security vulnerabilities** with appropriate security patches.

4. Monitoring of the Information Security Policy

The use of electronic and non-electronic information and the use of information systems shall be monitored for the following reasons:

- To ensure that this policy is adhered to and to detect and investigate unauthorised use of information
- To maintain the effectiveness, integrity and security of the computer network
- To ensure that the law is not being contravened
- To protect the services provided by the School and Council to the public and protect the integrity and reputation of the School and Council.

All monitoring shall be:

- Fair and proportionate to the risks of harm to the School and Council's information and reputation
- Undertaken so as to intrude on users' privacy only as much as is necessary
- Carried out similarly regardless of whether the user is office based or working remotely
- Carried out subject to the requirements of legislation, e.g. Regulation of Investigatory Powers Act 2000. Access to any records of usage shall be stringently controlled.

5. Review of the Information Security Policy

This policy shall be reviewed on a regular basis and at least annually. This policy and its associated policies, processes, procedures and guidelines shall be updated according to:

- Internally generated changes e.g. changes in service strategy, organisation, locations and technology
- Externally generated changes e.g. changes in legislation, security threats, security incidents, recommended best practice and audit reports
- All changes shall be approved by the Head Teacher and School Governors and be made available to everyone to whom it applies.

6 – Reporting Information Security Breaches

You must report security incidents and weaknesses to the following people:
Mr C Gliddon (Headteacher)
You can make your report by phone, face to face, using the online form or by letter - whichever you prefer.

Examples of incidents:

Breach of security

- Loss of computer equipment due to crime or an individual's carelessness
- Loss of computer media e.g. memory sticks
- Accessing any part of a database using someone else's authorisation either fraudulently or by accident
- Finding the doors and/or windows have been broken and forced entry gained to a secure room/building that contains service user records

Breach of confidentiality/security

- Finding a computer print out with a header and a person's information on it at a location outside of School premises
- Finding any paper records about a service user/member of staff or business of the organisation in any location outside of the School premises
- Being able to view service user records in the back (or front) of an employees car
- Discussing service user or staff personal information with someone else in an open area where the conversation can be overheard
- A fax being received by the incorrect recipient

7 – Passwords for Staff

1. Never reveal your password to anyone else or ask others for their password.

2. When choosing a password, choose a word or phrase that you can easily remember, but not something which can be used to identify you, such as your name or address. Generally, longer passwords are better than short passwords. It is advisable to use a 'strong' password. A strong password is one which contains a combination of upper and lower-case letters, numbers and other punctuation characters. You can substitute numbers and letters for other characters that look similar, such as '3' for 'E', '1' for 'I' or '@' for 'O', '!' for '1' etc. This will help to make your password much more difficult to guess. Remember that passwords are case-sensitive.

3. There is a useful tool that will help identify how strong a password you are using – check your password out at http://www.microsoft.com/protect/yourself/password/checker.mspx

4. Users with administrative level access should ensure that they utilise a complex password – 6 random character/numbers in mixed case.

5. If you forget your password, please request that it be reset from the System Administrator

6. If you believe that a student or other staff may have discovered your password, then change it ***immediately***

7. Never use the feature ‘Remember password’

8. Change passwords regularly

9. Never leave your computer unattended while using any personal data – if called away you should lock the workstation – this will normally require a password to reopen

10. Never allow another person to login to any system with your login ID and password. Auditing measures in place could result in you being responsible for the actions of another person. This is particularly risky in a situation where you as an adult allow a child to access materials under your login.

11. Never write your password down and leave it out for others to find.

8 – USB Memory Stick Policy / Removable Hardware

Despite their small size, USB memory sticks have a very large capacity and therefore pose a considerable security risk if they are lost, stolen or abused.

Oldfields Hall Middle school does allow the use of memory sticks but only if they are encrypted and supplied by the school. All other memory sticks, especially unencrypted, are banned

All removable hardware must be encrypted.

Importance of encryption, protection of equipment e.g. do not leave in a car or unattended.

9 – Use of personal devices i.e. Phone, iPads, laptops

All devices must be PIN / Password protected – staff to store securely.

10 - Email security

Unacceptable email activities, sending confidential information securely by email e.g. encryption. Personal use of school’s email system, security risk of personal internet based email accounts such as Yahoo and Hotmail. Staff to use only school email for work purposes.

11- Remote access security.

Accessing school’s data from outside the office best practice e.g. being careful about who can see the screen, making sure that all systems are logged out from before leaving the PC etc.

12 - Working from home security.

Protection of paper records: e.g. lock them away when not in use. Do not allow family or friends see school’s data. Family and friends should not use school’s ICT equipment.

13 - Protective Marking.

All data should be given a classification which will determine how it must be processed.

14 - Secure data transfer.

Encryption, approved mechanisms, receiving and recording authorisations for transferring data.

15 - Backups.

What should be backed up, frequency of backups, security of backup tapes and where they should be held etc.

16 - Printing/scanning/copier security.

Making sure that users make sure that confidential information (code to release) is not left in devices.

17 - Social Networking.

Detail what is classed as unacceptable behaviour, responsibility of staff to maintain confidentiality. The school's policy on having pupils or parents as friends etc. Code of conduct.

18 - Asset registers including data assets, hardware assets and software assets.

What should be recorded, who is responsible for recording etc. Relevant staff to log and update.

19 - Personal Network Storage/Cloud storage.

What the school's position is in allowing access to PNS sites. What if anything can be stored there. The use of cloud storage for school data etc.

20 - Clear desk policy.

Not leaving confidential papers lying on desks, using lockable filing cabinets etc.

21 - Process for allowing third parties access to school's systems.

E.g. Remote support, after school activities etc. Detail what assurances should be sought, what level of access should be given, what auditing should be in place etc.

22 - Physical security.

Make sure security badges are checked on arrival, visitors' credentials checked, windows and doors to secure areas kept locked. Sign in/out.

Declaration

I accept that I have a responsibility to safeguard Oldfields Hall Middle School information and equipment by abiding by the conditions of use defined in this Information Security Policy.

I understand that misuse of electronic and other communications may lead to consequences, which could be harmful to individuals, the Council, the School or other organisations. I understand that for certain types of misuse, I may be open to criminal prosecution under the Obscene Publications Act, the Computer Misuse Act or the Data Protection Act.

I understand that in order to ensure that the Information Security Policy is properly followed, and to maintain the effectiveness, integrity and security of the network, the use of electronic communications will be monitored.

Signed
Date

Appendix A – Glossary of Terms
This glossary contains definitions of information security terms used in this policy. If there are other terms which need defining, please xxxxxx

Accountability	The quality or state of being accountable, especially an obligation or willingness to accept responsibility or to account for one's actions. The ability to verifiably track actions to identifiable individuals.
Availability	Ensuring that authorised users have access to information and associated assets when required.
Confidentiality	Ensuring that information is accessible only to those authorised to have access.
Integrity	Safeguarding the accuracy and completeness of information and processing methods.
Information Security	The preservation of confidentiality, integrity, availability and accountability of information.
Information Security Risk Assessment	A structured method of analysing the risks to information. Risks consist of vulnerabilities (weaknesses) and threats. The selection of appropriate security controls is based on the likelihood of the risk occurring and the potential impact if the risk occurs.
Malicious Software	Any software written with the intention of doing damage, such as viruses, worms and spyware. The damage may be disclosure or loss of information, denial of access or making a computer unusable. Even if malicious software does no direct damage, covertly installed unauthorized software is still considered malicious.
PDA	Personal Digital Assistant – a small computing device used for diary management and e-mail.
Residual Risk	In general it is not possible or cost effective to remove all information risk - it might be technically impossible or not feasible on cost grounds. An understanding of the remaining "residual risk" allows it to be managed, for example by insurance. “Residual risk” is the level of risk that remains after controls have been introduced to manage the initial (inherent) risk.
Security Incidents and Weaknesses	A security incident (also called a security breach) is any event, which results in unauthorised access, loss, disclosure, modification or destruction of information whether accidental or deliberate. A security incident may not necessarily result in damage to information – it is still a breach of security. A security weakness is where there is potential for a security incident.
Structured Manual Filing Systems	Structured manual filing systems are called "relevant filing systems" in the Data Protection Act 1998, and are defined as “Any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible”.

Appendix B – Key Contacts

Owner and champion of the Information Security Policy

Job Title	Deputy Headteacher
Name	Victoria Marsh
E-mail address	V.Marsh@oldfields.staffs.sch.uk
Telephone no	01889-562770

System Administrator/ Network Manager:

Job Title	IT Support Officer
Name	Tim Wright
E-mail address	T.Wright@oldfields.staffs.sch.uk
Telephone no	01889-562770

SIMS System Administrator:

Job Title	IT Support Officer
Name	Tim Wright
E-mail address	T.Wright@oldfields.staffs.sch.uk
Telephone no	01889-562770

Responsible Person for Information Security within the school

Job Title	Deputy Headteacher
Name	Victoria Marsh
E-mail address	V.Marsh@oldfields.staffs.sch.uk
Telephone no	01889-562770

Responsible Person for Data Protection/Freedom of Information Requests

Job Title	Deputy Headteacher
Name	Victoria Marsh
E-mail address	V.Marsh@oldfields.staffs.sch.uk
Telephone no	01889-562770

Primary person to report a security breach or weakness to:

Job Title	Deputy Headteacher
Name	Victoria Marsh
E-mail address	V.Marsh@oldfields.staffs.sch.uk
Telephone no	01889-562770

Deputy person to report a security breach or weakness to:

Job Title	Headteacher
Name	Carl Gliddon
E-mail address	C.Gliddon@oldfields.staffs.sch.uk
Telephone no	01889-562770