DURHAM LANE

PRIMARY SCHOOL

Electronic Information Security Policy and Procedures
2023

Date Issued:	**February 2023**
Prepared by:	**Deputy Head Teacher**
Review date:	**February 2024**
Date Adopted by Governing Body:	**March 2024**
Signed	

This policy will be reviewed in 2024

This document contains important protocols and policy statements covering a range of Information Security protocols which are designed to support you in your day-to-day work, and protect both you and the school from security breech incidents. It is vital that you read this guide carefully and ensure that you understand your responsibilities in relation to Electronic Information Security.

Please remember that failure to comply with the protocols and policy, could have serious consequences and, depending upon the seriousness of the offence, could lead to disciplinary action or even dismissal and may result in legal claims against you and the school.

Employees must be aware of the need to preserve the confidentiality of information relating to pupils and other staff. Experience shows that the most likely breaches of confidentiality is sharing of information with people who don't need to know and that can include staff. Children, parents and members of staff have the right to expect that nothing about them is shared unless it is important to their welfare.

EMPLOYEE STATEMENT OF UNDERSTANDING

This Information Security Policy contains important protocols and policy statements covering a range of issues which are designed to support you in your day to day work, and protect both you and the School from security incidents.
It is vital that you read this guide carefully and ensure that you understand your responsibilities in relation to Information Security.

Occasionally there may be protocols which require changes to practices and procedures before they can be fully implemented and therefore you may not be able to comply with them. However, those staff who can adhere to these developing protocols will be expected to do so.

All employees are required to sign an **Electronic Information Security Statement of Understanding** acknowledging that they understand the information security protocols and policies and their responsibilities in relation to them.

Incident Reporting

Information security incident reporting is the effective feedback of actual, suspected or potential incidents to the appropriate person in school. If an incident occurs, it is important that it is reported to the appropriate person so that it can be addressed and dealt with before damaging the school or its employees.

An incident is any event that compromises directly or indirectly any aspect of information security, including breaches in information related legislation such as Data Protection and Copyright laws, affecting any combination of confidentiality, integrity, availability or legality. A **Security Incident Reporting Form** is available in school for recording any incidents.

Protocols

If you witness an information security incident:

- Report it immediately to the Head Teacher (the nominated person for reporting such incidents);
- Do not inform anyone who does not need to know;
- Do not attempt any investigation yourself as this could compromise evidence and could even make the situation worse;
- Ensure that you are familiar with the reporting procedures and definitions.

Advice and guidance

If you need further advice or guidance on any information security-related issue, contact the Head Teacher

The School's protocols in relation to Information Security are divided into the following sections:

1. Password Security
2. Visitor entry procedures
3. Clear desk security
4. Internet Use security
5. E-mail security
6. Fax and phone message security
7. Access/distribution of inappropriate material

This policy will be reviewed in 2024

8. Computer Network Security
9. Secure disposal of obsolete IT equipment
10. Prohibited use of Unauthorised software
11. Computer Virus Protection
12. Secure offsite use of IT equipment

1) Passwords

Passwords are a cost effective and simple way of controlling access to computer systems and the information held on them. A password system has two unique elements; the user-id which identifies you to the system, and a password which is a separate identification code which should only be known by you.

In exceptional circumstances, multi-user accounts are required in order to provide an efficient and effective service. These circumstances are rare, and the vast majority of users will have individual accounts and associated passwords.

Protocols

- Never disclose your password. If you give someone your password, you have given them your identity. As far as the system is concerned, anyone using your user-id and password is you, and anything they do is done by you. You will be held accountable.
- A password needs to be something that other people cannot easily guess, so avoid family names, car registrations, birthdays etc.
- Change any new password immediately on receipt.
- Commit your password to memory; never write it down.
- Change your password regularly, even if the system does not force you to.
- If your password is disclosed change it immediately.
- Create a new password every time you change; do not re-use old passwords or simply change a number in the password even if the system allows it.
- Never store passwords on a computer file.

Tips for thinking up good passwords

A good password is at least 7 characters long, is a mixture of letters and numbers and is difficult to guess but easy to remember. When thinking up passwords you could:

- *use the beginning or end letters of a phrase*
- *try substituting numbers for letters e.g. I becomes 1, S becomes 5*
- *take a word and spell it how it sounds*
- *for every letter in the word type the key directly above and to the left e.g. freedom becomes r433e9j*

1. Visitor Entry Procedures

We have clear access procedures in school. Managing visitors to school is a sign of courtesy and professionalism and is of course more for the security and protection of the children and staff working on the premises than for the protection of information and other assets. Visitors may not generally be a problem, but there are threats relating to visitors who could:

- view, access or steal sensitive information on notice boards, computer monitors or desks
- steal or damage equipment
- steal personal possessions
- plan a major theft

Protocols

- Visitors should be logged in and out and should wear a visitor's lanyard (Green for DBS visitors and red for all others) at all times.
- If you meet someone who is behaving suspiciously or who you suspect is an intruder, report it to reception / security. Be courteous, but sceptical – professional intruders are experts at being believable.
- Do not share door entry key codes.
- Encourage children to report visitors to a member of staff if they are not wearing a visitor's badge.

This policy will be reviewed in 2024

2. Clear Desk Security

Keeping your desk clear of sensitive material when you are away from it, is one of the most important contributions you can make to security. If information is left on view and documents and portable equipment left unattended, then there is a chance that they will be misused, mislaid or picked up by someone who should not have them. Please note that a 'Secure Desk' policy does not mean that you need to clear your desk every night; the policy only relates to the secure handling of confidential or sensitive information.

Protocols

- When using a PC for administration purposes or for assessments / report writing, the monitors can display sensitive information and can allow access to the main systems. Lock your terminal or log-off before leaving it unattended. Ensure that a password protected screensaver is active on your PC.
- Ensure USB and other removable media are properly stored away when not in use. Staff are only to use encrypted USBs for data protection reasons.
- Printed output should be cleared immediately and not left unattended on printers.
- Clear sensitive information from flip charts and other presentation equipment such as whiteboards.
- Mobile phones should be stored away in teacher cupboards
- Confidential files must be kept in secure storage.
- Documents and papers should always be filed when you are finished with them.
- Note pads or other media containing personal information should be kept secure at all times.
- In-trays and out-trays containing sensitive information should be secured before leaving them.
- Confidential or sensitive documents should be shredded or otherwise disposed of and not discarded in bins for ordinary waste.

3. Internet Use Security

This section contains some details of the School's Internet Usage protocols and policies. For full information please refer to the School Internet Use Policy.

Protocol

- The internet should only be accessed via the broadband and after authorisation by the Head Teacher.
- Access should only be made via the authorised account and password, the password should not be made available to any other person
- All internet use during school hours should be appropriate to staff professional activity or to student's education.
- The Internet should not be used for private purposes without permission from a senior member of staff. This should be completed in your own time.
- The school retains the right to restrict or remove personal access to the internet
- Use for personal financial gain, gambling, political purposes or advertising is forbidden
- Access to Internet sites of a dubious nature is forbidden, particularly in regard to sites involving material of a sexually explicit or violent nature and material which is offensive in any way. Accidental access to a dubious site or any site which you feel should be included in the restricted categories, or any access attempts which are blocked, must be reported to the Head Teacher (nominated person in school) and OneIT.
- Closed discussion groups can be useful, but the use of public chat rooms is not allowed.
- The school reserves the right to examine or delete any files that may be held on its computer systems and to monitor any Internet sites visited.
- All site access is automatically logged and regularly checked. Detailed access logs can be requested by the Head Teacher
- Ensure a password protected screen saver is active on your PC and that the time parameter is set to a reasonably short period, say 5 – 10 minutes.
- Copyright of materials and intellectual property rights must be respected
- Your Head Teacher can authorise the un-blocking of a site category for your use if this is pertinent to your job function.
- The security of the IT system must not be compromised whether owned by the school, by Stockton Borough Council or any other organisation or individual.

This policy will be reviewed in 2024

4. Email Security

This section contains the school's protocol and policies on the use of e-mail together with information on e-mail etiquette.

- E-mail facilities are available for business and educational use, with reasonable private usage being permitted, provided it does not interfere with your duties.
- Any E-mails that the user wishes to remain private must have this indicated in both the header and in the message box.
- E-mail usage is logged and monitored, and may be inspected at any time without notice.
- E-mail messages have to be disclosed in litigation. Before sending an email, ask yourself how you would feel if it was read out in court.
- Obtain confirmation of receipt of important emails that you send, together with a hard copy of all important emails sent and received.
- Check your email every working day and reply promptly to those requiring a response. Where a prompt detailed response is not possible, send an acknowledgement giving an estimate of when a full response will be sent.
- Do not impersonate any other person when using email.
- Do not amend messages received.
- Do not create congestion by sending trivial messages or personal messages or by copying emails to those who do not need to see them.
- Do not send or forward email messages or documents which are, or may be construed as harassment or bullying, defamatory, obscene, pornographic or sexually explicit.
- Do not send or forward email messages or documents which are, or may be construed as contractually binding to the school in any way.
- Do not send or forward email messages or documents which divulge information concerning another employees private affairs, without consent of the employee.
- Do not send or forward email messages or documents which contain confidential information
- Do not send or forward email messages or documents which would be in breach of the Data Protection Act 1998 or any other legislation restricting or controlling the disclosure of information.
- Do not utilise information obtained at work to further your private interests or those of your relatives or friends.
- Do not use any other person's email account.
- Our emails are not encrypted, so anything included in an email could be easily read by someone other than the intended recipient. It is important that sensitive or personal information is not sent to outside organisations via email unless they are password protected, and that internal emails should only contain sensitive or personal information where absolutely necessary.

Email etiquette

There are 3 reasons why email etiquette is required:

- **Professionalism:** by using proper email language we will convey a professional image;
- **Efficiency:** emails that get to the point are much more effective than poorly worded emails;
- **Protection from liability**: employee awareness of email risks will protect the school and the individual from legal action.

The most important etiquette rules are listed below. Following these rules will ensure that your emails are safe, efficient and effective.

- Be concise and to the point
- Answer all questions, and pre-empt further questions
- Use proper spelling, grammar and punctuation
- Answer swiftly
- Do not attach unnecessary files
- Use proper structure and layout
- Do not write in CAPITALS
- Do not leave out the message thread
- Add disclaimers to your emails
- Read the email before you send it
- Do not overuse Reply to All

This policy will be reviewed in 2024

- Take care with abbreviations and emoticons such as :-) used to represent a smiley face
- Be careful with formatting
- Do not copy a message or attachment without permission
- Use a meaningful subject
- Use active instead of passive
- Avoid using URGENT or IMPORTANT
- Avoid long sentences

5. Telephone Messages

Exchanging information by phone messages introduces the risk that information could be easily available to people other than the intended recipient.

- Take care what messages you leave on answer machines and voice mail.
- When exchanging personal or sensitive information over the phone, always verify the identity of the caller. If you are asked for information about a child, and you don't know the caller or have never spoken to them before, take down their number and call them back. DO NOT accept a mobile number; ask for the number of their place of work.
- Be aware of the dangers of providing information over the phone e.g. participating in telephone surveys. If you wish to take part in a telephone survey always verify the identity of the caller before providing information. It is recommended that you do not respond to telephone surveys; instead request an electronic or paper-based version of those you consider worthwhile.

6. Access/distribution of inappropriate Material

Anything that is offensive, illegal or not directly related to your work may be considered inappropriate. Obvious subjects considered to be offensive include pornography, racism, sexism and violence, but remember that there is a whole range of other issues which could be considered inappropriate. Also, be aware that inappropriate material can be held in many forms, not just electronically.

Sending, receiving or accessing inappropriate material could inflict damage and have serious consequences for yourself, your colleagues and the School, resulting in:

- legal liability and prosecution;
- bad publicity and damage to the image of the Authority;
- disciplinary proceedings against individuals;
- damage to professional relationships amongst employees;
- damage to working relationships with partner organisations.

Protocol

- Do not send, distribute or re-distribute inappropriate material.
- Do not access inappropriate material.
- If you receive inappropriate material, treat it as an Information Security Incident and report it immediately to the designated person.

7. Computer Network Security

The computer network is a single secure system monitored and protected in partnership with one IT the school service provider. In-built security features guard and protect the system as long as it remains unchanged. Staff are provided with levels of access to the system linked to their school role and responsibility. Each staff member has a personalised log in which includes the use of a user name and password. All activity within the network system can be monitored and reviewed by the service provider. This information must be held securely at all times. Never disclose your log in information to a third party.

8. Secure Disposal of Obsolete Equipment

There are a number of Information Security issues relating to the disposal of computer equipment. Whether the equipment is to be scrapped, re-cycled or used by another organisation care must be taken to avoid either unauthorised disclosure of information or accidental loss or destruction of information and physical equipment.

This policy will be reviewed in 2024

Protocol

- Clearly identify the equipment for disposal
- Ensure that the equipment does not have periodic, if infrequent, use.
- Always ensure that backup or archive data from the old system can be restored and read by the current system if required.
- Monitored control the removal of the equipment from the premises by One IT.
- Ensure that equipment is not on a current lease / rental agreement prior to disposal.
- Ensure equipment is removed from the asset register immediately after disposal.
- Be aware of and always adhere to the school equipment disposal procedure as there are regulations on this.

9. Use of Unauthorised Software

Unauthorised software, that is software which is not explicitly authorised, is one of the main causes of expensive computer crashes and wasted time. The use of unauthorised software is strictly forbidden as it introduces a range of dangers:

- Copyright – using unlicensed software is legally theft
- Viruses, which can damage both your own and the rest of the school's systems and data
- Shareware - it may need licensing after a trial period
- It could conflict with other systems or software causing failure or creating anomalies which could lead to exposing systems to risk
- Registry corruption – which often results in the PC having to be rebuilt

Typical examples of unauthorised software are games, shareware, private screensavers, internet downloads and unlicensed or borrowed software. For the purposes of this protocol, the term 'software' also includes all types of electronic files which are not specifically connected to or required for your normal day-to-day work-related activities.

Protocol

- Never load unauthorised software onto any school owned equipment.
- Any queries on what is unauthorised software in a school should be referred to the member of staff who holds the software licenses / master copies.
- Never install unauthorised software onto any equipment that may be attached to the school's network.

10. Computer Virus Protection

Viruses are malicious code which are introduced into computer systems. There are literally thousands of viruses in circulation, and your computer can be infected in a variety of ways, via:

- CDs and other electronic media which you use to exchange data
- any computer network your computer might be attached to
- the internet
- e-mail attachments
- shareware and freeware
- games and utilities
- magazine cover disks

Viruses are electronic vandalism and pose a very real and constant threat to information security. They are a major source of wasted time, effort and expense, and in some cases, if they are not found in time, could seriously damage the operational ability and reputation of the Authority.

Protocol

- OneIT to ensure anti-virus software is run regularly; ideally every day and ensure the use up-to-date anti-virus software on laptops, portable and stand-alone PC's.
- Only run authorised software.
- Only use media from known and trusted sources.
- Look out for and report anything strange.
- Do not attempt to fix a virus yourself.
- Expect the worst. If in doubt, seek advice from the schools' IT Helpdesk.

This policy will be reviewed in 2024

11. Secure offsite use of IT equipment

Using school IT equipment at home is permitted. Portable equipment is very convenient but it is more vulnerable as the normal school security procedures cannot protect the equipment when you are 'out and about'.

The obvious risks arising from the use of portable equipment include:

- loss of equipment and any information held on it;
- use of equipment in circumstances where confidential information may be overheard or viewed;
- theft, either for the equipment itself or because of the information held on it;
- damage by accident; in addition to the financial costs of repair or replacement, information held on the damaged equipment may be irretrievable.

Portable equipment is anything that is owned by the school and is issued to you to enable you to do your job whilst away from your office or work place. These includes laptop computers, IPads and mobile phones that are the property of the school.

Protocol

- Teachers / support staff have full use of loaned laptops to support their work
- Where a laptop computer has been made available to a member of staff on a long-term loan, they are free to install software appropriate to their professional needs providing all the appropriate licences are kept securely
- Where a laptop computer has been made available to a member of staff on a long-term loan, no restrictions or barriers are placed on home Internet access provided that the device is not then connected to the school network. Members of staff are free to choose their own ISP and are responsible for any charges incurred.
- The protocols in the Guide to Information Security apply equally to the home use of School equipment. This includes the use of virus protection software, the seeking out of inappropriate / offensive materials on the Internet and the use of personal IDs and passwords.
- Laptop computers in particular have a high re-sale value and they should not be left in cars or in a place where an opportunist could take it. With most insurance companies laptops are covered in cars as long as they are not left unattended.
- School employees should be aware that they are aware of the arrangements that have been made by the school for insurance cover on portable equipment and to follow any guidelines / procedures established by the school to safeguard this cover.
- Employees should be aware of the school's policy on the use of laptops and the school network
- Make sure that you know how to use the equipment.
- Ensure that equipment left unattended is securely stored and out of sight.
- Be careful in busy or crowded locations; people may be able to view or overhear confidential information.
- Do not advertise your valuables.
- Always make back-up copies of important information and ensure these are held securely

Legislation

There is a great deal of legislation which may affect you and your work, and it must be remembered that ignorance is no defence. However, individual and collective legal responsibilities will be covered in the Authority's protocols, policies and procedures, and if you adhere to these, then you will not be in danger of breaking the law.

The principle laws relating to information security are summarised below.

- The Data Protection Act 1998 protecting against illegal disclosure and use of personal data.
- The Freedom of Information Act 2000 giving a general right of access to all types of recorded information held by public authorities
- The Electronic Communications Act 2000 ensuring safe and secure electronic commerce.
- The Regulation of Investigatory Powers Act 2000 updating the law with respect to the interception of communications.
- The Misuse of Computers Act 1990 making it an offence to gain unauthorised access to a computer, computer systems and the information they contain.
- The Copyright, Designs and Patents Act 1988 making it an offence to make unauthorised copies of software packages.
- The Copyright and Rights in Databases Regulations 1997 specifically addressing database ownership rights.
- The Defamation Act 1996 covering the publication of defamatory material.

This policy will be reviewed in 2024

- The Human Rights Act 1998 dealing with a person's private rights.

Remember, you do not need to know the legal requirements of these acts in detail. By simply following the School's protocols, policies, and procedures you will guarantee your compliance.

Information Back Up and Recovery

It is essential that the data stored on the school's central servers is backed-up daily as in an emergency it can usually be recovered. As any data stored on the hard drive of individual PC's or on any electronic device other than the central servers is not included in the standard back-up and recovery procedures, it is your responsibility to ensure that any important data not stored on central servers is appropriately protected from loss or damage. If you need any advice or guidance on how to back-up your data please contact One IT Helpdesk.

Protocol

- Wherever possible, store important data on the School's centrally controlled servers.
- Ensure that important data held on remote servers are protected by appropriate back-up and recovery procedures.
- Ensure that important data held on individual PC's or other stand-alone devices are protected by appropriate back-up and recovery procedures.

Changes to policy:
2023

- Pg 3 visitors' badges replaced by a visitor's lanyard (Green for DBS visitors and red for all others) at all times.

This policy will be reviewed in 2024

Electronic Information Security Statement of Understanding 2023 - 24

I confirm that I have read and fully understand the information security protocols and policies contained in the attached policy and that I also understand my responsibilities with regard to them.

I accept that Governors and Senior Leaders reserve the right to amend the protocols and policies. In the event of such amendments I will be appropriately notified, and a copy of the revised protocols and policies will be made available to me.

With regard to any future amendments or additions to information security protocols and policies, it is the responsibility of Governors and Senior Leaders to ensure that I am notified and provided with access to the amended protocols and/or policies. It is my responsibility to ensure that I read and understand them. Any material changes to protocols and policies will be subject to the usual consultation procedures.

Name: …….

Post: …….

Signature: ……. Date: ……

This policy will be reviewed in 2024

Security Incident – Report

SI Number:
Date of incident:
Date incident was reported/investigation started:
Incident reported by:
Incident reported to:

Additional staff/customers/suppliers involved:

Summary

- Enter a summary here

Action Details – First Response

- Enter a summary of initial corrective steps taken

Action Details – Security Incident Raised

- Enter summary of the information raised

Action Details – Investigation

- Give details of any logs used, any reporting systems and export these logs or PST's / One Drives etc, they may be needed later. Give details of these below

Action Details - Outcome

- Give details of the outcome and specifics on how you come to this conclusion

Remediation Actions – One IT

- Give details of any follow up actions / changes that will be made to mitigate or prevent future incidents (One IT Specific)

This policy will be reviewed in 2024

Remediation Actions –

- Give details of any follow up actions / changes that will be made to mitigate or prevent future incidents (One IT Specific)

Additional Notes / Technical Details

- Give details of any backups taken, e.g. a PST, any logs exported etc and either attach the logs to the document in zip format or reference where the PST / Backups etc can be found. Also list any other relevant info