1Excellence
Multi Academy Trust

Whatever you do, work at it with all your heart.
Colossians 2:23

St Mark's C of E Primary School

Information Security Policy

- **Approved by governors: (date)**

Reviewed: January 2018

To be reviewed: January 2019

Information Security Policy

Mission Statement

At St Mark's C of E Primary School we will:

- Welcome everyone
- Build Christian values and worship into our teaching
- Establish strong links between home, school and community
- Endeavour to reach our full potential and celebrate our achievements
- Care for, encourage and respect each other
- Support each other to stay safe, healthy and make a positive contribution to our World

Our school is a place where every person has the right to be themselves and to belong and learn in a safe and happy environment. Everyone at our school is equal and treats each other with respect and kindness. We do not tolerate bullying.

The need for information security

The significant increase in the value and availability of information over recent years has brought with it increased information security risks. Advances in technology have resulted in a new information culture, and proper controls need to be established in order to safeguard our business activities, ensure our legal compliance and protect our image and credibility.

1.1 Structure of the guide

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

- Passwords
- Visitor entry control
- Incident reporting
- Secure desk policy
- Internet
- E-mail
- Fax and phone messages
- Inappropriate material
- Hardware
- Disposal of obsolete equipment
- Unauthorised software
- Viruses
- Mobile / offsite working

- The law
- Back-up and recovery

The protocols support the School's Information Security Policy.

1.2 General responsibilities

1.2.1 This document contains important protocols and policy statements covering a range of Information Security 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.

1.2.2 From time to time the protocols and policy may be amended or new ones published. When this happens it is the responsibility of Management to make you aware of the changes and to provide you with access to the amended documents. In turn it is your responsibility to ensure that you read and understand them.

1.2.3 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.

1.2.4 Employees at all times should 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.

1.3 Statement of Understanding

All employees are required to sign a Statement of Understanding acknowledging that they understand the information security protocols and policies and their responsibilities in relation to them (see section 17).

1.4 Advice and guidance

If you need any further advice or guidance on any information security related issue you can contact your line manager or the Headteacher

2. Passwords

2.1 Introduction

2.1.1 If used correctly 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.

2.1.2 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. For multi-user account users the protocols still apply; the phrases *you* and *your* relating to the group of authorised users and not the individual.

2.2 Protocols

Ref	Protocol
01	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.
02	A password needs to be something that other people cannot easily guess, so avoid family names, car registrations, birthdays etc.
03	Change any new password immediately on receipt.
04	Commit your password to memory; never write it down.
05	Change your password regularly, even if the system does not force you to.
06	If your password is disclosed change it immediately.
07	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.
08	Never store passwords on a computer file.

2.3 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 eg 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 eg freedom becomes r433e9j

3. Visitor entry controls

3.1 Introduction

3.1.1 We have door access controls around the building to keep out unwanted visitors.

3.1.2 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

3.2 Protocols

Ref	Protocol
01	Your visitors are your responsibility.
02	Visitors should be logged in and out.
03	Visitors should wear a visitor's pass at all times.
04	Always wear your ID badge (if issued)
05	If you meet someone who is behaving suspiciously or who you suspect is an intruder report it to reception / security.
06	Be courteous but sceptical – professional intruders are experts at being believable.
07	Do not disclose door entry codes.

3. Visitor entry controls

4. Incident reporting

4.1 Introduction

4.1.1 Information security incident reporting is the effective feedback of actual, suspected or potential information security incidents via the appropriate channels. If an information security 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.

4.1.2 Prevention is better than cure, and it is preferable to identify potential problems before they become actual incidents. Remember that minor problems are easier to deal with than major ones, and early fixes are generally easier and less expensive.

4.2 Definition

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.

4.3 Incident Reporting Form

An Incident Reporting Form is available in school for recording any incidents

4.4 Protocols

If you witness an information security incident:

Ref	Protocol
01	Report it immediately to the Headteacher or Deputy Headteacher
02	Do not inform anyone who does not need to know.
03	Do not attempt any investigation yourself as this could compromise evidence and could even make the situation worse.
04	Know the procedure. Ensure that you are familiar with the reporting procedures and definitions.
05	Follow the checklist. Ensure that you follow the procedure, even if it looks easy.

5. Secure desk policy

5.1 Introduction

5.1.1 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.

5.1.2 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.

5.2 Protocols

Ref	Protocol
01	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.
02	Ensure that removable media e.g. memory sticks are properly stored away when not in use.
03	Printed output should be cleared immediately and not left unattended on printers or fax machines.
04	Clear sensitive information from flip charts and other presentation equipment such as whiteboards.
05	Never leave mobile phones or PDA's unattended.
06	Confidential files must be kept in secure storage.
07	Documents and papers should always be filed when you are finished with them.
08	Note pads or other media containing personal information should be kept secure at all times.
09	In-trays and out-trays containing sensitive information should be secured before leaving them.
10	Confidential or sensitive documents should be shredded or otherwise disposed of and not discarded in bins for ordinary waste.

6. Internet

6.1 Introduction

This section contains details of the School's Internet Usage protocols and policies.

6.2 Protocols

Ref	Protocol
01	The internet should only be accessed via the broadband and after authorisation by your Headteacher.
02	Access should only be made via the authorised account and password, the password should not be made available to any other person
03	All internet use during school hours should be appropriate to staff professional activity or to student's education.
04	The Internet may be used for private purposes in your own time following guidelines established by the school.
05	The School retains the right to restrict or remove personal access.
06	Use for personal financial gain, gambling, political purposes or advertising is forbidden
07	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 by the Northern Grid for Learning's or Stockton Borough Council's monitoring software, must be reported to the Headteacher and the Schools' IT Helpdesk.
08	Closed discussion groups can be useful but the use of public chat rooms is not allowed.
09	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.
10	All site access is automatically logged and regularly checked. Detailed access logs can be requested by the Headteacher
11	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.
12	Copyright of materials and intellectual property rights must be respected
13	Your Headteacher can authorise the un-blocking of a site category for your use if this is pertinent to your job function.
14	The security of the ICT system must not be compromised whether owned by the school, by Stockton Borough Council or any other organisation or individual.

7. e-mail

7.1 Introduction

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

7.2 Protocols

Ref	Protocol
01	E-mail facilities are available for business and educational use, with reasonable private usage being permitted provided it does not interfere with your duties.
02	Any E-mails that the user wishes to remain private must have this indicated in both the header and in the message box.
03	E-mail usage is logged and monitored, and may be inspected at any time without notice.
04	E-mail messages have to be disclosed in litigation. Before sending an e-mail ask yourself how you would feel if it was read out in court.
05	Obtain confirmation of receipt of important e-mails that you send, together with a hard copy of all important e-mails sent and received.
06	Check your e-mail 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.
07	Do not impersonate any other person when using e-mail.
08	Do not amend messages received.
10	Do not create congestion by sending trivial messages or personal messages or by copying e-mails to those who do not need to see them.
11	Do not send or forward e-mail messages or documents which are, or may be construed as harassment or bullying, defamatory, obscene, pornographic or sexually explicit.
12	Do not send or forward e-mail messages or documents which are, or may be construed as contractually binding to the School in any way.
13	Do not send or forward e-mail messages or documents which divulge information concerning another employees private affairs without consent of the employee.
14	Do not send or forward e-mail messages or documents which contain confidential information
15	Do not send or forward e-mail 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.
16	Do not utilise information obtained at work to further your private interests or those of your relatives or friends.
17	Do not use any other persons e-mail account.
18	Our e-mails are not encrypted, so anything included in an e-mail 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 e-mail, and that internal e-mails should only contain sensitive or personal information where absolutely necessary.

7.3 e-mail etiquette

7.3.1 Why do we need e-mail etiquette?

There are 3 reasons why e-mail etiquette is required :

- professionalism **: by using proper e-mail language we will convey a professional image**
- efficiency **: e-mails that get to the point are much more effective than poorly worded e-mails**
- **protection from liability** : employee awareness of e-mail risks will protect the Authority and the individual from legal action

7.3.2 Etiquette rules

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

1. Be concise and to the point
2. Answer all questions, and pre-empt further questions
3. Use proper spelling, grammar and punctuation
4. Make it personal
5. Use templates for frequently used responses
6. Answer swiftly
7. Do not attach unnecessary files
8. Use proper structure and layout
9. Do not overuse the high priority option
10. Do not write in CAPITALS
11. Do not leave out the message thread
12. Add disclaimers to your e-mails
13. Read the e-mail before you send it
14. Do not overuse Reply to All
15. Take care with abbreviations and emoticons such as :-) used to represent a smiley face
16. Be careful with formatting
17. Do not copy a message or attachment without permission
18. Use a meaningful subject
19. Use active instead of passive
20. Avoid using URGENT or IMPORTANT
21. Avoid long sentences
22. Make appropriate use of the ‘out-of-office’ facility

8. Phone and fax messages

8.1 Introduction

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

8.2 Protocols

Ref	Protocol
01	When sending fax messages always re-check the number you have dialled before transmission.
02	When sending faxes make sure that the person you are sending confidential information to is there to receive it.
03	Treat any fax message received in error as highly confidential, return it to the sender and do not divulge it's contents to anyone else.
04	Take care what messages you leave on answer machines and voice mail.
05	When exchanging personal or sensitive information over the phone, always verify the identity of the caller.
06	Do not use the School's equipment to send or respond to junk faxes without approval from your line manager.
07	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.

9. Inappropriate material

9.1 Introduction

9.1.1 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.

9.1.2 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

9.2 Protocols

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

10. Hardware

10.1 Introduction

10.1.1 You need to think of our computer networks and software as a single secure system. In-built security features guard and protect the system as long as it remains unchanged. However, even a small change which is not properly managed can create a weakness, exposing the system and what it contains to a potential security risk.

10.1.2 Using non-approved hardware and connections introduces a range of dangers :

- it could cause your equipment to fail
- it could invalidate warranties on your equipment
- it could undermine your system's security controls by creating new routes into the system

10.2 Protocols

Ref	Protocol
01	Never tamper with or make unauthorised changes to any system.
02	Never install hardware or software without proper authorisation.
03	Always refer any query or problem with the system to the school technician or the Schools' ICT Helpdesk.
04	Never try to rectify a problem yourself unless authorised and qualified to do so.

11. Disposal of obsolete equipment

11.1 Introduction

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.

11.2 Protocols

Ref	Protocol
01	Clearly define the equipment for disposal.
02	Ensure that the equipment does not have periodic, if infrequent, use.
03	Always ensure that backup or archive data from the old system can be restored and read by the current system if required.
04	Closely control the removal of the equipment from the premises.
05	Ensure that equipment is not on a current lease / rental agreement prior to disposal.
06	Ensure equipment is removed from the asset register immediately after disposal.
07	Be aware of and always adhere to the School's equipment disposal procedure as there are regulations on this.

12. Unauthorised software

12.1 Introduction

12.1.1 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
- if it is 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

12.1.2 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.

12.2 Protocols

Ref	Protocol
01	Never load unauthorised software onto any School owned equipment.
02	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.
03	Never install unauthorised software onto any equipment that may be attached to the School's network.

13. Viruses

13.1 Introduction

13.1.1 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, memory sticks and any 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

13.1.2 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.

13.2 Protocols

Ref	Protocol
01	Always follow the School policies and procedures.
02	Make sure that your anti-virus software is run regularly; ideally every day.
03	Always use up-to-date anti-virus software on laptops, portable and stand-alone PC's.
04	Only run authorised software.
05	Only use media from known and trusted sources.
07	Look out for and report anything strange.
08	Do not attempt to fix a virus yourself.
09	Expect the worst.
10	If in doubt, seek advice from the Schools' IT Helpdesk.

14. Mobile working

4.1 Introduction

4.1.1 Using school IT equipment at home is now commonplace. 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'.

4.1.2 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.

4.2 Definition

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 portable/laptop computers, electronic organisers and PDA's (palmtops, pocket PC's etc), mobile phones and pagers, and projectors and display equipment. Computers provided under the Laptops for Teachers Scheme are the property of the School.

4.3 Protocols

Ref	Protocol
01	Teachers / support staff frequently have full use of loaned laptops to develop planning, curriculum subject and ICT experience
02	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
03	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.
04	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 i.d.s and passwords.
05	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.
06	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.
07	Employees should be aware of the school's policy on the use of laptops and the school network
08	Make sure that you know how to use the equipment.
09	Ensure that equipment left unattended is securely stored and out of sight.
10	Be careful in busy or crowded locations; people may be able to view or overhear confidential information.
11	Do not advertise your valuables.
12	Always make back-up copies of important information and ensure these are held securely

15. The law

15.1 Introduction

15.1.1 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.

15.1.2 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 a 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.

- **The Human Rights Act 1998** dealing with a persons private rights.

15.1.3 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.

16. Back-up and recovery

16.1 Introduction

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 the Schools' ICT Helpdesk.

16.2 Protocol

Ref	Protocol
BU01	Wherever possible store important data on the School's centrally controlled servers.
BU02	Ensure that important data held on remote servers are protected by appropriate back-up and recovery procedures.
BU03	Ensure that important data held on individual PC's or other stand-alone devices are protected by appropriate back-up and recovery procedures.

St Mark's C of E Primary School

EMPLOYEE STATEMENT OF UNDERSTANDING

The Employees Guide to Information Security 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.

STATEMENT OF UNDERSTANDING

I confirm that I have read and fully understand the information security protocols and policies contained in the Employees Guide to Information Security, and that I also understand my responsibilities with regard to them.

I accept that Management 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 Management 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.

16. Back-up and recovery

Name .....

Post

Signature .....

Date .....

Approved
……

Date……
……