St Martin’s CE Primary School

E-Safety and Data Protection Policy

Introduction

Computer technology in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- ✓ Websites
- ✓ Learning Platforms and Virtual Learning Environments
- ✓ E-mail and Instant Messaging
- ✓ Chat Rooms and Social Networking
- ✓ Blogs and Wikis
- ✓ Podcasting
- ✓ Video Broadcasting
- ✓ Music Downloading
- ✓ Gaming
- ✓ Mobile/ Smart phones with text, video and/ or web functionality
- ✓ Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At the Ivory Federation, we understand the responsibility to educate our children on eSafety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Schools hold personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of our schools. This can make it more difficult for your school to use technology to benefit learners.

Everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and children) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, personal digital assistants (or Tablets), tablets, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by children and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, Tablets and portable media players, etc).

Monitoring

Authorised ICT staff (ICT Technician), Headteacher or Data Protection Officer may inspect any ICT equipment owned or leased by the School at any time without prior notice. If you are in doubt as to whether the individual requesting such access is authorised to do so, please confirm their eligibility with the Headteacher.

ICT authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain School business related information; to confirm or investigate compliance with School policies, standards and procedures; to ensure the effective operation of School ICT; for quality control or training purposes; to comply with a Subject Access Request under the General Data Protection Register 2018 (GDPR), or to prevent or detect crime.

ICT authorised staff may, without prior notice, access the e-mail or voice-mail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the General Data Protection Register 2018 (GDPR), the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

Please note that personal communications using School ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

Breaches

A breach or suspected breach of policy by a School employee, contractor or pupil may result in the temporary or permanent withdrawal of School ICT hardware, software or services from the offending individual.

Any policy breach is grounds for disciplinary action in accordance with the School Disciplinary Procedure or, where appropriate, the Oldham / Ivory Federation Disciplinary Procedure or Probationary Service Policy.

Policy breaches may also lead to criminal or civil proceedings.

The procedures for managing breaches is fully outlined in the school's Data Protection and Privacy Policy.

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's DPO or Headteacher. Additionally, all security breaches, lost/stolen equipment or data (including USB flash pens), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the DPO and Headteacher with immediate effect (within 24 hours).

Computer Viruses

All files downloaded from the Internet, received via e-mail or on removable media (e.g. floppy disk, CD, USB stick) must be checked for any viruses using school provided anti-virus software before using them.

Never interfere with any anti-virus software installed on school ICT equipment that you use.

If your machine is not routinely connected to the school network, you must make provision for regular virus updates through the ICT Technician.

If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact your ICT support provider immediately. The ICT support provider will advise you what actions to take and be responsible for advising others that need to know.

Data Security

The accessing and appropriate use of school data is something that the school takes very seriously. The expectations of staff are fully outlined in the school's Data Protection and Privacy Policy.

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 will be issued with the relevant guidance documents and the Policy for ICT Acceptable Use.

Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight.

Staff should always carry portable and mobile ICT equipment or removable media as hand luggage, and keep it under your control at all times.

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. Our federation uses the following coding :

Low Confidentiality Status	Moderate Confidentiality Status	High / Significant Confidentiality Status

Apply labelling in accordance with guidance from your Data Protection Officer (DPO).

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.

Data Protection Officer (DPO)

The DPO in this school is provided by Justin Hardy who is employed by Oldham LA. Full details and contact information are available on the school's website.

The role of the DPO 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 DCSF 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 of

As a result, the DPO is able to manage and address risks to the information and make sure that information handling complies with legal requirements laid down in the GDPR (2018).

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.

Disposal of Redundant ICT Equipment Policy

All redundant ICT equipment will be disposed off through an authorised agency or via the Oldham LA disposal scheme. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.

All redundant ICT equipment that may have held personal data will have the storage media over written multiple times to ensure the data is irretrievably destroyed. Or if the storage media has failed it will be physically destroyed. We will only use authorised companies who will supply a written guarantee that this will happen.

Disposal of any ICT equipment will conform to:
The Waste Electrical and Electronic Equipment Regulations 2006

The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007
http://www.environment-agency.gov.uk/business/topics/waste/32084.aspx
http://www.opsi.gov.uk/si/si2006/uksi_20063289_en.pdf
http://www.opsi.gov.uk/si/si2007/pdf/uksi_20073454_en.pdf?lang=_e

General Data Protection Register 1998
http://www.ico.gov.uk

Electricity at Work Regulations 1989
http://www.opsi.gov.uk/si/si1989/Uksi_19890635_en_1.htm

The school will maintain a comprehensive inventory of all its ICT equipment including a record of disposal.

The school's disposal record will comply with the Oldham guidance and be within the delegated limits as defined by the schools Governors

**** if personal data is likely to be held the storage media will be over written multiple times to ensure the data is irretrievably destroyed.***

Any redundant ICT equipment being considered for sale / gift will have been subject to a recent electrical safety check and hold a valid PAT certificate.

Further information is available at:

Waste Electrical and Electronic Equipment (WEEE) Regulations Environment Agency web site Introduction

http://www.environment-agency.gov.uk/business/topics/waste/32084.aspx

The Waste Electrical and Electronic Equipment Regulations 2006

http://www.opsi.gov.uk/si/si2006/uksi_20063289_en.pdf

The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007

http://www.opsi.gov.uk/si/si2007/pdf/uksi_20073454_en.pdf?lang=_e

Information Commissioner website
http://www.ico.gov.uk/

Mail

The use of e-mail within most schools is an essential means of communication for both staff and children. In the context of school, e-mail should not be considered private.

Educationally, e-mail can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that children need to understand how to style an e-mail in relation to their age and good network etiquette ; 'netiquette'. In order to achieve the KS2 computing expectations, children must have experienced sending and receiving e-mails.

Managing e-Mail

The school gives all / most staff their own e-mail account to use for all school business as a work based tool. This is to minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed.

It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The school email account should be the account that is used for all school business.

Under no circumstances should staff contact children, parents, clients or conduct **ANY** school business using personal e-mail addresses.

The school requires a standard disclaimer to be attached to all e-mail correspondence, stating that, 'the views expressed are not necessarily those of the school or the LA'. The responsibility for adding this disclaimer lies with the account holder. The disclaimer text to be added in our schools is as follows :

Confidentiality: This email and its contents and any attachments are intended only for the above named. As the email may contain confidential or legally privileged information, if you are not, or suspect that you are not, the above named or the person responsible for delivery of the message to the above named, please delete or destroy the email and any attachments immediately.

Security and Viruses: This note confirms that this email message has been swept for the presence of computer viruses. However, we advise that in keeping with good management practice, the recipient should ensure that the email together with any attachments are virus free by running a virus scan themselves. We cannot accept any responsibility for any damage or loss caused by software viruses.

Monitoring: The school undertakes monitoring of both incoming and outgoing emails. You should therefore be aware that if you send an email to a person within the school it may be subject to any monitoring deemed necessary by the organisation from time to time. The views of the author may not necessarily reflect those of the school.

Access as a public body: The school may be required to disclose this email (or any response to it) under the Freedom of Information Act, 2000, the Data Protection Act or the GDPR requirements unless the information in it is covered by one of the exemptions in the Act.

Legal documents: The school does not accept service of legal documents by email.

All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper.

Staff sending e-mails to external organisations, parents or children are advised to cc. the Headteacher, line manager or designated account holder.

Governors, trustees or directors should ensure that they **ONLY** use the provided school e-mail address when communicating on school related business.

Children may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.

E-mails created or received as part of your School job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your e-mail account as follows:

- Delete all e-mails of short-term value
- Organise e-mail into folders and carry out frequent house-keeping on all folders and archives

All pupil e-mail users are expected to adhere to the generally accepted rules of netiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments.

Children must immediately tell a teacher/ trusted adult if they receive an offensive e-mail.

Staff must inform (the DPO or Headteacher) if they receive an offensive e-mail.

Children are introduced to e-mail as part of the Computing Scheme of Work.

However you access your school e-mail (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply

The use of Hotmail, Googlemail, AOL, Outlook Online or any other Internet based webmail service for sending, reading or receiving business related e-mail is not permitted in any circumstances.

Sending e-Mails

If sending e-mails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, refer to the Section e-mailing Personal, Sensitive, Confidential or Classified Information.

ONLY EVER Use your own school e-mail account so that you are clearly identified as the originator of a message.

If you are required to send an e-mail from someone else's account, always sign on through the 'Delegation' facility within your e-mail software so that you are identified as the sender (if available within your software).

Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate.

Do not send or forward attachments unnecessarily. Whenever possible, send the location path to a password protected 'folder' in a cloud based account rather than sending attachments.

An outgoing e-mail greater than ten megabytes (including any attachments) is likely to be stopped automatically. This size limit also applies to incoming e-mail

School e-mail is not to be used for personal advertising.

Receiving e-Mails

- Check your e-mail regularly
- Activate your 'out-of-office' notification when away for extended periods
- Use the 'Delegation' facility within your e-mail software so that your e-mail can be handled by someone else while you are not at work (if available within your software)
- Never open attachments from an untrusted source; Consult your network manager first.
- Do not use the e-mail systems to store attachments. Detach and save business related work to the appropriate shared drive/folder.
- The automatic forwarding and deletion of e-mails is not allowed.

E-mailing Personal, Sensitive, Confidential or Classified Information

Assess whether the information can be transmitted by other secure means before using e-mail.
The use of Hotmail, Gmail, AOL or any other Internet based webmail service for sending e-mail containing sensitive information is not permitted.

Where your conclusion is that e-mail must be used to transmit such data:

- Obtain express consent from your manager to provide the information by e-mail
- Exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:
- Verify the details, including accurate e-mail address, of any intended recipient of the information
- Verify (by phoning) the details of a requestor before responding to e- mail requests for information
- Do not copy or forward the e-mail to any more recipients than is absolutely necessary
- Do not send the information to any body/person whose details you have been unable to separately verify (usually by phone)
- Send the information as an encrypted document attached to an e-mail
- Provide the encryption key or password by a separate contact with the recipient(s)
- Do not identify such information in the subject line of any e-mail
- Request confirmation of safe receipt

In Addition …
When sending an e-mail containing personal or sensitive data you need to put a security classification in the first line of the e-mail. For e-mails to do with information about a pupil, for example, you need to put in PROTECT – PERSONAL on the first line of the e-mail.

This also needs to go on the top of any documents that you send (i.e. Word documents, Reports, Forms, including paper documents you send in hardcopy, etc). The name of the individual is not to be included in the subject line and the document containing the information encrypted. This provides additional security.

Equal Opportunities

Children with Additional Needs : The school endeavours to create a consistent message with parents for all children and this in turn should aid establishment and future development of the schools' e-Safety rules.

However, staff are aware that some children may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of eSafety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of eSafety. Internet activities are planned and well managed for these children and young people.

eSafety

eSafety - Roles and Responsibilities

As eSafety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named eSafety co-ordinator in this school is the Headteacher who has been designated this role as a member of the senior leadership team. All members of the school community have been made aware of who holds this post. It is the role of the eSafety co-ordinator to keep abreast of current issues and guidance through organisations such as Oldham LA, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and Governors are updated by the Head/ eSafety co-ordinator and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and children, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home–school agreements, and behaviour/pupil discipline (including the anti-bullying) policy and PSHE.

eSafety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for eSafety guidance to be given to the children on a regular and meaningful basis. eSafety is embedded within our curriculum and we continually look for new opportunities to promote eSafety.

- The school has a framework for teaching internet skills in ICT lessons.

- The school provides opportunities within a range of curriculum areas to teach about eSafety

- Educating children on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the eSafety curriculum

- Children are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them

- Children are taught about copyright and respecting other people's information, images, etc through discussion, modelling and activities

- Children are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Children are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline or CEOP report abuse button

- Children are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the computing curriculum

eSafety Skills Development for Staff

Our staff receive regular information and training on eSafety issues in the form of on-line references, INSET or staff meetings.

New staff receive information on the school's acceptable use policy as part of their induction.

All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of eSafety and know what to do in the event of misuse of technology by any member of the school community.

All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas.

Managing the School eSafety Messages

- We endeavour to embed eSafety messages across the curriculum whenever the internet and/or related technologies are used.

- The eSafety policy will be introduced to the children at the start of each school year.

- eSafety posters will be prominently displayed.

Misuse and Infringements

Complaints

Complaints and/ or issues relating to eSafety should be made to the eSafety co- ordinator or Headteacher. Incidents should be logged and where necessary / appropriate referred to the relevant agency in accordance with personnel or safeguarding procedures.

Inappropriate Material

All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the eSafety co-ordinator.

Deliberate access to inappropriate materials by any user will lead to the incident being logged by the eSafety co-ordinator, depending on the seriousness of the offence; investigation by the Headteacher/ LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.

Users are made aware of sanctions relating to the misuse or misconduct as defined in the Personnel Handbook and within the trust's personnel guidelines.

Internet Access

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All use of is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

Managing the Internet

The school maintains children who will have supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet technology.

- Staff will preview any recommended sites before use
- Raw image searches are discouraged when working with children
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.

All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.

All users must observe copyright of materials from electronic resources.

Temporary users will also need to comply with the Acceptable Use Policy.

Internet Use

You must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise its intended restricted audience.

Don't reveal names of colleagues, customers or clients or any other confidential information acquired through your job on any social networking site or blog.

On-line gambling or gaming is not allowed on school owned equipment or through the LA internet services.

It is at the Headteacher's discretion on what internet activities are permissible for staff and children and how this is disseminated.

Infrastucture

Oldham LA Local Authority has a monitoring solution via the Oldham LA Grid for Learning where web-based activity is monitored and recorded.

School internet access is controlled through the LA’s web filtering service.

Our school also employs some additional web filtering which is the responsibility of the ICT Technician

St Martin’s is aware of its responsibility when monitoring staff communication under current legislation and takes into account; General Data Protection Register (2018), The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998.

Staff and children are aware that school-based email and internet activity can be monitored and explored further if required.

The school does not allow children access to internet logs.

The school uses management control tools for controlling and monitoring workstations.

If staff or children discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the e-safety coordinator or teacher as appropriate.

It is the responsibility of the school, by delegation to the network manager, to ensure that Anti-virus protection is installed and kept up-to-date on all school machines.

Children and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school’s responsibility nor the network manager’s to install or maintain virus protection on personal systems. If children wish to bring in work on removable media it must be given to the ICT Technician for a safety check first.

Staff should seek to avoid the use of portable, removeable data devices e.g. USB stick, portable hard drive. They should instead seek to use online cloud based services. However, if it is essential that staff use removable media that is protected, via the use of a password / encrypted device.

Children and staff are not permitted to download programs or files on school based technologies without seeking prior permission from the ICT Technician.

If there are any issues related to viruses or anti-virus software, the network manager should be informed.

Managing Other Web 2 Technologies

Web 2, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However, it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our children to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

At present, the school endeavours to deny access to social networking sites to children within school.

All children are advised to be cautious about the information given by others on sites, for example users not being who they say they are.

Children are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.

Children are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests).

Our children are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.

Children are encouraged to be wary about publishing specific and detailed private thoughts online.

Our children are asked to report any incidents of bullying to the school.

Staff may only create blogs, wikis or other web 2 spaces in order to communicate with children using systems approved by the Headteacher.

Parental Involvement

We believe that it is essential for parents/ carers to be fully involved with promoting eSafety both in and outside of school and also to be aware of their responsibilities. We regularly consult and discuss eSafety with parents/ carers and seek to promote a wide understanding of the benefits related to ICT and associated risks.

Parents/ carers and children are actively encouraged to contribute to adjustments or reviews of the school eSafety policy.

Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school.

Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g., on school website).

Parents/ carers are expected to sign a Home School agreement containing the following statement or similar …..

→ We will support the school approach to on-line safety and not deliberately upload or add any images, sounds or text that could upset or offend any member of the school community

The school disseminates information to parents relating to eSafety where appropriate in the form of;

- ✓ Information and celebration evenings
- ✓ Posters
- ✓ Website/ Learning Platform postings
- ✓ Newsletter items
- ✓ Learning platform training

Passwords and Password Security

Passwords

- ✓ Always use your own personal passwords to access computer based services
- ✓ Make sure you enter your personal passwords each time you logon
- ✓ Do not include passwords in any automated logon procedures
- ✓ Staff should change temporary passwords at first logon
- ✓ Change passwords whenever there is any indication of possible system or password compromise
- ✓ Do not record passwords or encryption keys on paper or in an unprotected file
- ✓ Only disclose your personal password to authorised ICT support staff when necessary, and never to anyone else
- ✓ Ensure that all personal passwords that have been disclosed are changed once the requirement is finished
- ✓ Passwords should contain a minimum of six characters and be difficult to guess
- ✓ User ID and passwords for staff and children who have left the School are removed from the system within one week

If you think your password may have been compromised or someone else has become aware of your password report this to the ICT Technician.

Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The children are expected to keep their passwords secret and not to share with others, particularly their friends. Staff and children are regularly reminded of the need for password security.

All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-safety Policy and Data Security.

Users are provided with an individual network, email, Learning Platform and Management Information System (where appropriate) log-in username.

Children are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others

Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, MIS systems and/or Learning Platform, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked.

Due consideration should be given when logging into the Learning Platform to the browser/cache options (shared or private computer).

In our school, all ICT password policies are the responsibility of the Headteacher and all staff and children are expected to comply with the policies at all times.

Zombie Accounts

Zombie accounts refers to accounts belonging to users who have left the school and therefore no longer have authorised access to the school's systems. Such Zombie accounts when left active can cause a security threat by allowing unauthorised access.

Ensure that all user accounts are disabled once the member of the school has left (within one week).

Prompt action on disabling accounts will prevent unauthorised access.

Regularly change generic passwords to avoid unauthorised access (©Microsoft advise every 42 days)

Personal or Sensitive Information

Protecting Personal, Sensitive, Confidential and Classified Information

- Ensure that any School information accessed from your own PC or removable media equipment is kept secure

- Ensure you lock your screen before moving away from your computer during your normal working day to prevent unauthorised access

- Ensure the accuracy of any personal, sensitive, confidential and classified information you disclose or share with others

- Ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person

- Ensure the security of any personal, sensitive, confidential and classified information contained in documents you fax, copy, scan or print. This is particularly important when shared mopiers (multi-function print, fax, scan and copiers) are used and when access is from a non-school environment

- Only download personal data from systems if expressly authorised to do so by your manager

- You must not post on the internet personal, sensitive, confidential, or classified information, or disseminate such information in any way that may compromise its intended restricted audience

- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information

- Ensure hard copies of data are securely stored and disposed of after use in accordance with the document labeling

Storing/Transferring Personal, Sensitive, Confidential or Classified Information Using Removable Media

Where possible, we advise against the use of portable devices, instead recommending the use of online cloud services. But, where they are to be used :

- Ensure removable media is purchased with encryption
- Store all removable media securely
- Securely dispose of removable media that may hold personal data
- Encrypt all files containing personal, sensitive, confidential or classified data
- Ensure hard drives from machines no longer in service are removed and stored securely or wiped clean

Remote Access

- You are responsible for all activity via your remote access facility
- Only use equipment with an appropriate level of security for remote access
- To prevent unauthorised access to School systems, keep all access information such as telephone numbers, logon IDs and PINs confidential and do not disclose them to anyone
- Select PINs to ensure that they are not easily guessed, e.g. do not use your house or telephone number or choose consecutive or repeated numbers
- Avoid writing down or otherwise recording any network access information. Any such information that is written down must be kept in a secure place and disguised so that no other person will be able to identify what it is
- Protect School information and data at all times, including any printed material produced while using the remote access facility. Take particular care when access is from a non-School environment
- It will be considered a disciplinary offence to 'access the network remotely' without seeking permission from the Headteacher

School ICT Equipment

As a user of ICT, you are responsible for any activity undertaken on the school's ICT equipment provided to you.

✓ It is recommended that schools log ICT equipment issued to staff and record serial numbers as part of the school's inventory.

✓ Do not allow your visitors to plug their ICT hardware into the school network points (unless special provision has been made). They should be directed to the wireless ICT Facilities if available.

✓ Ensure that all ICT equipment that you use is kept physically secure.

✓ Do not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990

- ✓ It is imperative that you save your data on a frequent basis. You are responsible for the backup and restoration of any of your data that is not held on the school's network drive

- ✓ Personal or sensitive data should not be stored on the local drives of desktop PCs. If it is necessary to do so the local drive must be encrypted

- ✓ It is recommended that a time locking screensaver is applied to all machines. Any PCs etc accessing personal data must have a locking screensaver as must any user profiles

Privately Owned ICT Equipment Should Not Be Used On A School Network
On termination of employment, resignation or transfer, return all ICT equipment to your Manager.

You must also provide details of all your system logons so that they can be disabled.

It is your responsibility to ensure that any information accessed from your own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person.

All ICT equipment allocated to staff must be authorised by the appropriate Line Manager. Authorising Managers are responsible for:

- maintaining control of the allocation and transfer within their area of responsibility

  recovering and returning equipment when no longer needed
- All redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and General Data Protection Register (GDPR)

Portable & Mobile ICT Equipment
This section covers such items as laptops, Tablets and removable data storage devices. Please refer to the relevant sections of this document when considering storing or transferring personal or sensitive data.

All activities carried out on School systems and hardware will be monitored in accordance with the general policy.

Staff must ensure that all school data is stored on school's network, and not kept solely on the laptop.

Any equipment where personal data is likely to be stored must be encrypted.

Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey.

Synchronise all locally stored data, including diary entries, with the central school network server on a frequent basis.

Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades.

The installation of any applications or software packages must be authorised by the ICT support team, fully licensed and only carried out by your ICT support.

In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight.

Portable equipment must be transported in its protective case if supplied.

Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, Tablets, gaming devices, mobile and Smart phones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use.

Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile Devices (including phones)

The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil, parent/ carer, fellow professional or other 'client' using their personal device.

- ✓ Children are allowed to bring personal mobile devices/phones to school but must not use them for personal purposes within lesson time. At all times the device must be switched onto silent

- ✓ This technology may be used, however for educational purposes, as mutually agreed with the Headteacher. The device user, in this instance, must always ask the prior permission of the bill payer

- ✓ The school is not responsible for the loss, damage or theft of any personal mobile device

- ✓ The sending of inappropriate text messages between any member of the school community is not allowed

- ✓ Permission must be sought before any image or sound recordings are made on these devices of any member of the school community

- ✓ Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device

School Provided Mobile Devices (including phones)

- The sending of inappropriate text messages between any member of the school community is not allowed
- Permission must be sought before any image or sound recordings are made on the devices of any member of the school community

- Where the school provides mobile technologies such as phones, laptops and Tablets for offsite visits and trips, only these devices should be used
- Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school

Removable Media

If storing/transferring personal, sensitive, confidential or classified information using Removable Media please refer to the section 'Storing/Transferring Personal, Sensitive, Confidential or Classified Information Using Removable Media'.

- Only use recommended removable media
- Store all removable media securely
- Removable media must be disposed of securely by your ICT support team

Servers

Newly installed servers holding personal data should be encrypted, therefore password protecting data. SIMs Database Servers installed by SITSS since April 2009 are supplied with encryption software.

- ✓ Always keep servers in a locked and secure environment
- ✓ Limit access rights
- ✓ Always password protect and lock the server
- ✓ Existing servers should have security software installed appropriate to the machine's specification
- ✓ Back up tapes (where still in use) should be encrypted by appropriate software
- ✓ Data must be backed up regularly
- ✓ Back up tapes/discs must be securely stored in a fireproof container (where still in use)
- ✓ Back up media stored off-site must be secure
- ✓ Remote back ups should be automatically securely encrypted

Systems and Access

You are responsible for all activity on school systems carried out under any access/account rights assigned to you, whether accessed via school ICT equipment or your own PC.

Do not allow any unauthorised person to use school ICT facilities and services that have been provided to you.

Use only your own personal logons, account IDs and passwords and do not allow them to be used by anyone else.

Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information.

Ensure you lock your screen before moving away from your computer during your normal working day to protect any personal, sensitive, confidential or otherwise classified data and to prevent unauthorised access.

Ensure that you logoff from the PC completely when you are going to be away from the computer for a longer period of time.

Do Not Introduce or Propagate Viruses

It is imperative that you do not access, load, store, post or send from school ICT any material that is, or may be considered to be, illegal, offensive, libellous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the school or may bring the school or OLDHAM into disrepute. This includes, but is not limited to, jokes, chain letters, files, emails, clips or images that are not part of the school's business activities; sexual comments or images, nudity, racial slurs, gender specific comments, or anything that would offend someone on the basis of their age, sexual orientation, religious or political beliefs, national origin, or disability (in accordance with the Sex Discrimination Act, the Race Relations Act and the Disability Discrimination Act).

Any information held on School systems, hardware or used in relation to School business may be subject to The Freedom of Information Act.

Where necessary, obtain permission from the owner or owning authority and pay any relevant fees before using, copying or distributing any material that is protected under the Copyright, Designs and Patents Act 1998.

It is essential that any hard drives which may have held personal or confidential data are 'scrubbed' in way that means the data can no longer be read. It is not sufficient to simply delete the files or reformat the hard drive. Whoever you appoint to dispose of the equipment must provide a written guarantee that they will irretrievably destroy the data by multiple over writing the data.

Telephone Services

You may make or receive personal telephone calls provided:

- They are infrequent, kept as brief as possible and do not cause annoyance to others
- They are not for profit or to premium rate services
- They conform to this and other relevant OLDHAM and school policies.

School telephones are provided specifically for school business purposes and personal usage is a privilege that will be withdrawn if abused.

Be aware that the laws of slander apply to telephone calls. Whilst a telephone call may seem to have a temporary and private existence it still qualifies as admissible evidence in slander law cases.

Ensure that your incoming telephone calls can be handled at all times.

Follow the appropriate procedures in the event of receiving a telephone call containing a bomb threat. These procedures should be made readily available throughout your office. If you do not have a copy, please ask your line manager.

Mobile Phones

You are responsible for the security of your school mobile phone. Always set the PIN code on your school mobile phone and do not leave it unattended and on display (especially in vehicles) Report the loss or theft of any school mobile phone equipment immediately.

The school remains responsible for all call costs until the phone is reported lost or stolen.

You must read and understand the user instructions and safety points relating to the use of your school mobile phone prior to using it.

School SIM cards must only be used in school provided mobile phones.

All school mobile phones are barred from calling premium rate numbers and any numbers outside of the UK as the default.

You must not send text messages to premium rate services.

In accordance with the Finance policy on the private use of School provided mobiles, you must reimburse the school for the cost of any personal use of your school mobile phone. This includes call charges incurred for incoming calls whilst abroad. [To assist you in identifying personal use, add * to the end of the number being contacted, these will be shown separately on your bill]. Payment arrangements should be made through your finance administrator.

Never use a hand-held mobile phone whilst driving a vehicle. Only genuine 999 or 112 emergency calls may be made if it would be unsafe to stop before doing so.

Review Procedure

There will be an on-going opportunity for staff to discuss with the eSafety coordinator any issue of eSafety that concerns them.

There will be an on-going opportunity for staff to discuss with the SIRO/AIO any issue of data security that concerns them.

This policy will be reviewed every (12) months and consideration given to the implications for future whole school development planning.

The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.

This policy has been read, amended and approved by the staff, head teacher and governors in March 2018.

St Martin’s CE Primary Staff, Governor and Visitor
Acceptable Use Agreement / Code of Conduct

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Headteacher.

- ✓ I will only use the school’s email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed ‘reasonable’ by the Head or Governing Body
- ✓ I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
- ✓ I will ensure that all electronic communications with children, staff and parents / clients are compatible with my professional role
- ✓ I will not give out my own personal details, such as mobile phone number and personal e- mail address, to children or other ‘client’
- ✓ I will only use the approved, secure e-mail system(s) for any school business
- ✓ I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely
- ✓ Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off site must be encrypted
- ✓ I will not install any hardware of software without permission of the ICT Technician
- ✓ I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory
- ✓ Images of children and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher
- ✓ I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
- ✓ I will respect copyright and intellectual property rights
- ✓ I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute
- ✓ I will support and promote the school’s e-Safety and Data Security policies and help children to be safe and responsible in their use of ICT and related technologies
- ✓ I understand this forms part of the terms and conditions set out in my contract of employment (where appropriate)

User Signature

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school.

Signature : ***Date :***

Full Name : ***Job Title :***