ICT SECURITY

Mottram CE Primary School believes that IT plays an important part in both teaching and learning over a range of subjects.

Mottram CE Primary School is committed to ensuring that both staff and pupils have access to the necessary facilities and support to allow them to carry out their work.

This policy covers the rules and procedures for authorised and unauthorised use of the IT and communication facilities and is implemented in conjunction with the school's IT & E-safety Policy.

This information contains:

- The school's view on the use of e-mail and the internet at work.
- An explanation on what you can or cannot do.
- The consequences if you fail to follow the rules set out in this policy.
- General information relating to IT, including the Data Protection Act.
- The IT Technicians duties to the IT policy.

Policy

- The use of the IT facilities within the school is encouraged, as its appropriate use facilitates communication and can improve efficiency.
- Used correctly, it is a tool that is of assistance to employees. Its inappropriate use, however, can cause many problems, ranging from minor distractions to exposing the school to financial, technical, commercial and legal risks.
- Staff should always be an example of good practice to the students, serving as a positive role model in every aspect.
- Abuse of the IT facilities could result in the facilities being removed. Staff should always be aware of IT use, and misuse of the facilities, as defined in this policy, must be reported to the Headteacher.
- Since IT facilities are also used by students, there should be a policy outlining their use of facilities.
- Staff should make sure that pupils comply with that policy.
- Pupils misusing the IT facilities must be reported to the Headteacher.
- This policy applies to any computer connected to the school's network and computers.
- Any breach of the rules in this policy may result in disciplinary action, which may lead to dismissal.

- A misuse or breach of this policy could also result in criminal or civil actions being brought against the persons involved or the school.

Procedure

- The school's e-mail system and internet connection are available for communication and use on matters directly concerned with school's business.
- Employees using the school's e-mail system and internet connection should give particular attention to the following points in this policy.
- E-mail should not be used as a substitute for face-to-face communication, unless it is otherwise impossible.
- "Flame-mails" (e-mails that are abusive) can be a source of stress and can damage work relationships.
- Hasty messages, sent without proper consideration, can cause unnecessary misunderstanding.
- If an e-mail is confidential, the user must ensure that the necessary steps are taken to protect confidentiality.
- The school will be liable for any defamatory information circulated either within the school or to external contacts.
- The school's e-mail system and accounts must never be registered or subscribed to unsolicited e-mail (SPAM).
- Never disclose any of the school's e-mail addresses without confirming that they will not be subjected to SPAM and that they will not be sold on to marketing companies.
- All e-mails that are sent or received must be retained within the school for a period of six months.
- All e-mails being sent to external recipients must contain the school's standard confidentiality notice. This notice is normally configured as a signature by the IT technician and must not be removed.
- Non-text e-mails (containing graphics or colour) and e-mail attachments may contain harmful materials and computer viruses, which can seriously affect the IT facilities. If unsure, seek assistance or approval from the IT technician.
- Offers or contracts sent via e-mail or the internet are as legally binding as those sent on paper. An exchange of e-mails can lead to a contract being formed between the sender, or the school's and the recipient. Never commit the school to any obligations by e-mail or the internet without ensuring that you have the authority to do so. If you have any concerns, contact the Headteacher.

- Online purchases are only permitted with the Headteacher's authorisation, in order to comply with monitoring and accountability. Hard copies of the purchase must be made, for the purchaser and the finance manager. Any failure to follow these procedures satisfactorily may result in disciplinary action, including summary dismissal.

Authorised use of the IT facilities

The IT facilities should only be used as required by your work duties. This includes, but may not be limited to:

- Preparing work for lessons, activities, meetings, reviews, etc.
- Researching for any school related task
- Any school encouraged tuition or educational use
- Collating or processing information for school business
- Personal e-mail accounts are only permitted to be used if they have built-in anti-virus protection approved by the IT technician. Access to your personal e-mail must never interfere with your work duties.

Authorised use of the communications facilities

The communication facilities should only be used as required by your work duties.

This includes, but may not be limited to:

- Preparing work for lessons, activities, meetings, reviews, etc.
- Researching for any school related task
- Any school encouraged tuition or educational use
- If unsure about your required use, please seek authorisation from the Headteacher.

Unauthorised use of the IT facilities

It is not permitted under any circumstance to:

- Use the IT facilities for commercial or financial gain without the explicit written authorisation from the Headteacher.

- Physically damage the IT facilities.

- Re-locate, take off-site, or otherwise interfere with the IT facilities without the authorisation of the IT technician or Headteacher. Certain items are asset registered and security marked; their location is recorded by the financial assistant for accountability. Once items are moved after authorisation, staff have a responsibility to notify the financial assistant of the new location. The exception to this point is when items are moved to the designated secure room for insurance purposes over holiday periods.

- Use or attempt to use someone else's user account. All users of the IT facilities will be issued with a unique user account and password. The password must be changed at

regular intervals. User account passwords must never be disclosed to or by anyone. This is illegal under the Computer Misuse Act.

Use the IT facilities at any time to access, download, send, receive, view or display any of the following:

- Any material that is illegal
- Any message that could constitute bullying, harassment (including on the grounds of sex, race, religion/religious belief, sexual orientation or disability) or any negative comment about other persons or organisations
- Remarks relating to a person's sexual orientation, gender assignment, religion, disability or age
- Online gambling
- Remarks, which may adversely affect the reputation of any organisation or person, whether or not you know them to be true or false
- Any sexually explicit content

- Generate messages or documents that appear to originate from someone else, or otherwise impersonate someone else.
- Install hardware or software without the consent of the IT technician or the Headteacher.
- Introduce any form of stand-alone software or removable hardware likely to cause malfunctioning of the IT facilities or that will bypass, over-ride or overwrite the security parameters on the network or any of the school's computers. This is illegal under the Computer Misuse Act.
- Use or attempt to use the school's IT facilities to undertake any form of piracy, including the infringement of software licenses or other copyright provisions whether knowingly or not. This is illegal.
- Purchase any IT facilities without the consent of the IT technician or Headteacher. This is in addition to any purchasing arrangements followed according to school policy.
- Use or attempt to use the school's phone lines for internet or email access unless given authorisation by the Headteacher. This includes using or attempting to use any other form of hardware capable of telecommunication, regardless of ownership.
- Use any chat-lines, bulletin boards or pay-to-view sites on the internet. In addition, you must not download or attempt to download any software.
- Use the internet for any auctioning activity or to purchase items unless given authority to do so by the Headteacher. This is in addition to any purchasing arrangement followed according to school policy.

- Knowingly distribute or introduce a virus or harmful code onto the school's network or computers. Doing so may result in disciplinary action, including summary dismissal.

- Use the IT facilities for personal use without the authorisation of the Headteacher. This authorisation must be requested on each occasion of personal use.
- Copy, download or distribute any material from the internet or e-mail that may be illegal to do so. This can include computer software, music, text, and video clips. If it is not clear that you have permission to do so, or if the permission cannot be obtained, do not do so.
- To obtain and post on the internet, or send via e-mail, any confidential information about other employees, the school its customers or suppliers.
- Interfere with someone else's use of the IT facilities.
- Be wasteful of IT resources, particularly printer ink, toner and paper.
- Use the IT facilities when it will interfere with your responsibilities to supervise students.

- Any unauthorised use of e-mail or the internet is likely to result in disciplinary action including summary dismissal.
- If you are subjected to, or know about harassment or bullying, you are encouraged to report this immediately to your line senior or the Headteacher.

Unauthorised use of the communications facilities

It is not permitted under any circumstance to:

- Use the communication facilities for commercial or financial gain without the explicit written authorisation from the Headteacher.
- Physically damage the communication facilities.
- Use the communication facilities for personal use without authorisation from the Headteacher with the exception of the circumstance in 7.2.
- Re-locate, take off-site or otherwise interfere with the communication facilities without the authorisation of the Headteacher.
- Use the communication facilities at any time to access, receive, view or display any of the following:

- Any material that is illegal
- Any material that could constitute bullying, harassment (including on the grounds of sex, race religion/religious belief, sexual orientation or disability) or any negative comment about other persons or organisations
- Remarks relating to a person's sexual orientation, gender assignment, religion, disability or age

- Remarks, which may adversely affect the reputation of any organisation or person, whether or not you know them to be true or false
- Any sexually explicit material
- Any adult or chat-line phone numbers

- Use or attempt to use the school's communication facilities to undertake any form of piracy, including the infringement of media rights or other copyright provisions whether knowingly or not. This is illegal.

- Use or attempt to use the school's communication facilities for internet or e-mail access unless given authorisation by the Headteacher. This includes using or attempting to use any other form of hardware capable of telecommunication regardless of ownership.

- Copy, record or distribute any material from or with the communication facilities that may be illegal. This can include television media, films, telephone conversations and music. If it is not clear that you have permission to do so, or if the permission cannot be obtained, do not do so.

- Use or attempt to use the communication facilities to call overseas without the authorisation of the Headteacher.

- Use the communication facilities when it will interfere with your responsibilities to supervise students.

- Use of the school's telephone facilities for personal use is permitted for necessary calls lasting less than 10 minutes. Should you need to use the telephones for longer than this, then authorisation must be sought from the headteacher. This authorisation must be requested on each occasion. The exception to authorisation is the use of the telephone system to make personal emergency calls. However, the duty head or headteacher must be notified after the call. Any personal use of the telephones may be subject to a charge; this is at the Headteacher's discretion.

- Certain items are asset registered and security marked, their location is recorded by the financial assistant for accountability. Once items are moved following authorisation, staff have a responsibility to notify the financial assistant of their new location. The exception to this point is when items are moved to the designated secure room for insurance purposes over holiday periods.

- If you are subjected to or know about harassment or bullying, you are encouraged to report to your line senior or Headteacher.

Implementation of the policy

- Regular monitoring and recording of e-mail messages will be carried out on a random basis. Hard copies of e-mail messages can be used as evidence in disciplinary proceedings.

- Use of the telephone system is logged and monitored.
- Use of the school's internet connection is recorded and monitored.
- The Finance Manager randomly checks asset registered and security marked items.
- The IT technician checks computer logs on the schools network regularly.
- Unsuccessful and successful log-ons are logged on every computer connected to the school's network.
- Unsuccessful and successful software installations, security changes and items sent to the printer are also logged.
- The IT technician can remotely view or interact with any of the computers on the school's network. This may be used randomly to implement the IT Policy and to assist in any difficulties.
- The school's network has anti-virus software installed with a centralised administration package; any virus found is logged to this package.
- The school's database systems are computerised you must not access the system. Failure to adhere to this requirement may result in disciplinary action.
- All users of the database system will be issued with a unique individual password, which must be changed at regular intervals. Do not, under any circumstances, disclose this password to any other person.
- Attempting to access the database using another employee's user account/password without prior authorisation is likely to result in disciplinary action, including summary dismissal.
- User accounts are accessible by the Headteacher and the IT technician.
- Users must ensure that critical information is not stored solely within the school's computer system. Hard copies must be kept or stored separately on the system. If necessary, documents must be password protected.
- Users are required to be familiar with the requirements of the Data Protection Act 1998, and to ensure that they operate in accordance with the requirements of the Act. The obligations under the Act are complex but employees must adhere to the following rules:

- Do not disclose any material about a person, including a pupil, without their permission
- Such material includes information about a person's racial or ethnic origin, sex life, political beliefs, physical or mental health, trade union membership, religious beliefs, financial matters and criminal offences

- Do not send any personal data outside the UK

General IT Information

- Messages should be deleted after six months or stored in a suitable hard copy file.
- Information and data on the school's network and computers should be kept in an organised manner and should be placed in a location of an appropriate security level.
- If unsure, please seek help and information from the IT technician.
- Employees who feel that they have cause for complaint as a result of e-mail communications should raise the matter initially with their line senior or Headteacher, as appropriate. The complaint can then be raised through the grievance procedure.

IT technician's duties

To monitor and affect accountability of the IT policy, the IT technician is required to:

- Carry out regular daily checks on internet activity of all user accounts and to report any inappropriate use to the line manager/Headteacher.
- Monitor the computer logs on the school's network and to report any logged inappropriate use to the line manager/Headteacher.
- Remotely view or interact with any of the computers on the school's network. This may be done randomly to implement the IT policy and to assist in any difficulties.
- Access files and data to solve problems for a user, with their authorisation. If an investigation is requested by the Headteacher, authorisation from the user is not required.
- Adjust access rights and security privileges in the interest of the protection of the school's data, information, network and computers.
- Disable user accounts of staff that do not follow the policy, at the request of the headteacher.
- Assist the Headteacher in all matters requiring reconfiguration of security and access rights and in all matters relating to the IT Policy.

Assist staff with authorised use of the IT facilities, if required.

Document attached to the E-Safety and ICT Policies