Poplar Street Primary School
ICT Security and Acceptable Use Policy

Including E-Safety Policy

2016

Working Together – Aiming High!

Contents

1. Introduction

1.1. The purpose of the Policy is to protect the institution's information assets from all threats, whether internal or external, deliberate or accidental.

1.2. It is the policy of Poplar Street Primary School to ensure that:

- information will be protected against unauthorised access
- confidentiality of information will be assured
- integrity of information will be maintained
- regulatory and legislative requirements will be met
- business continuity plans will be produced, maintained and tested
- ICT security training will be available to all staff

2. Policy Objectives

2.1. Against this background there are three main objectives of the ICT Security Policy:

- to ensure that equipment, data and staff are adequately protected against any action that could adversely affect the school;
- to ensure that users are aware of and fully comply with all relevant legislation;
- to create and maintain within the school a level of awareness of the need for ICT security to be an integral part of the day to day operation so that all staff understand the need for ICT security and their own responsibilities in this respect.

3. Application

3.1. The ICT Security Policy is intended for all school staff who are either controllers of the system or who are users and supporters of the school's administration and curriculum ICT systems or data. Pupils using the school's ICT systems or data are covered by the school's 'Acceptable Use Policy' documents.

3.2. For the purposes of this document the terms 'ICT' (or 'ICT system'), 'ICT data' and 'ICT user' are defined as follows:

- 'ICT' (or 'ICT system') means any device or combination of devices used for the storage or processing of data and includes: workstation (netbook, notebook, desktop/tower PC), PDA, cash till, server or any other similar device;
- 'ICT data' means any information stored and processed within the ICT system and includes programs, text, pictures and sound;
- 'ICT user' applies to any School or Council employee, pupil or other authorised person who uses the school's ICT systems and/or data.

4. Roles and Responsibilities

4.1. The ICT Security Policy relies on management and user actions to ensure that its aims are achieved. Consequently, roles and responsibilities are defined below.

4.2. Governing Body

- The governing body has the ultimate corporate responsibility for ensuring that the school complies with the legislative requirements relating to the use of ICT systems and for disseminating policy on ICT security and other ICT related matters. These documents can be found at http://www.tamesideschoolssupport.net. In practice, the day-to-day responsibility for implementing these legislative requirements rests with the Headteacher.

4.3. Headteacher

- The Headteacher is responsible for ensuring that the legislative requirements relating to the use of ICT systems are met and that the school's ICT Security Policy, as may be amended from time to time, is adopted and maintained by the school. He/she is also responsible for ensuring that any special ICT security measures relating to the school's ICT facilities are applied and documented as an integral part of the Policy.
- In practice, the day to day functions should be delegated to the 'System/Network Manager', who must be nominated in writing by the Headteacher. This would take the form of an item in a job description.
- The Headteacher is responsible for ensuring that the requirements of the Data Protection Act 1998 are complied with fully by the school. This is represented by an on-going responsibility for ensuring that the :
    - registrations under the Data Protection Act are up-to-date and cover all uses being made of personal data and
    - registrations are observed with the school.
- In addition, the Headteacher is responsible for ensuring that users of systems and data are familiar with the relevant aspects of the Policy and to ensure that the appropriate controls are in place for staff to comply with the Policy. This is particularly important with the increased use of computers and laptops at home. Staff should exercise extreme care in the use of personal data at home to ensure legislation is not contravened, in particular the Data Protection Act 1998.

4.4. School Technician

- The school technician at Poplar Street is 'the System Manager' and is responsible for the school's ICT equipment, systems and data and will have direct control over these assets and their use, including responsibility for controlling access to these assets and for defining and documenting the requisite level of protection. The System Manager will be an employee of the school.
- The System Manager will administer the practical aspects of ICT protection and ensure that various functions are performed, such as maintaining the integrity of the data, producing the requisite back-up copies of data and protecting the physical access to systems and data.
- In line with these responsibilities, the System Manager will be the official point of contact for ICT security issues and as such is responsible for notifying the Headteacher or Chair of Governors of any suspected or actual breach of ICT security occurring within the school. The Headteacher or Chair of Governors should ensure that details of the suspected or actual breach are recorded and made available to Internal Audit upon request. The Headteacher or Chair of Governors must advise Internal Audit of any suspected or actual breach of ICT security pertaining to financial irregularity.
- It is vital, therefore, that the System Manager is fully conversant with the ICT Security Policy and maintains an up to date knowledge of best practice and follows the associated approved practices.

4.5. School Technician

- The school technician is responsible for maintaining, repairing and proactively supporting the ICT System so that it can meet the requirements of the ICT Security Policy. The School Technician will respond to actions delegated by the head teacher in order to ensure that the ICT System can comply with the ICT Security Policy.
- The school technician will also monitor the ICT System for breaches of security and inform the Headteacher.

4.6. Users

- Users are those employees, pupils or authorised guests of the school who make use of the ICT system to support them in their work. All users of the school's ICT systems and data must comply with the requirements of this ICT Security Policy. The school has an Acceptable Use Policy which summarises the responsibilities of users of the school's ICT systems.
- Users are responsible for notifying the System Manager of any suspected or actual breach of ICT security. In exceptional circumstances, users may report any such breach directly to the Headteacher, Chair of Governors or to Tameside MBC Internal Audit department.
- Users are responsible for the equipment they use including:
    - Physical security
    - Virus updates
    - Operating system updates
    - Security of data
    - Their own passwords.

5. Management of the Policy

5.1. Sufficient resources should be allocated each year to ensure the security of the school's ICT systems and to enable users to comply fully with the legal requirements and policies covered in this policy. If insufficient resources are available to fully implement this policy, then the potential risks must be documented and reported to Governors by the Headteacher.

5.2. Suitable training for all ICT users and documentation to promote the proper use of ICT systems will be provided. Users will also be given adequate information on the policies, procedures and facilities to help safeguard these systems and related data. A record of the training provided through the school to each individual user will be maintained. Maintenance of this record should be the responsibility of the nominated 'Network/System Manager'.

5.3. In addition, users will be made aware of the value and importance of such ICT systems and data, particularly data of a confidential or sensitive nature, and be made aware of their personal responsibilities for ICT security.

5.4. To help achieve these aims, the relevant parts of the ICT Security Policy and any other information on the use of particular facilities and techniques to protect the systems or data will be disseminated to users.

5.5. The Headteacher must ensure that adequate procedures are established in respect of the ICT security implications of personnel changes. Suitable measures should be applied that provide for continuity of ICT security when staff vacate or occupy a post. These measures as a minimum must include:

- a record that new staff have been issued with, have read the appropriate documentation relating to ICT security, and have signed the list of rules;
- a record of the access rights to systems granted to an individual user and their limitations on the use of the data in relation to the data protection registrations in place;
- a record that those rights have been amended or withdrawn due to a change to responsibilities or termination of employment.

6. Physical Security

6.1. Location Access

- Adequate consideration should be given to the physical security of rooms containing ICT equipment (including associated cabling). As far as practicable, only authorised persons should be admitted to rooms that contain servers or provide access to data. The server rooms should be locked when left unattended. Ideally, such rooms should have a minimum of key pad access.
- The System Manager must ensure appropriate arrangements are applied for the removal of any ICT equipment from its normal location. These arrangements should take into consideration the risks associated with the removal and the impact these risks might have.

6.2. Equipment siting

- Reasonable care must be taken in the siting of computer screens, keyboards, printers or other similar devices. Wherever possible, and depending upon the sensitivity of the data, users should observe the following precautions:
  - devices are positioned in such a way that information stored or being processed cannot be viewed by persons not authorised to know the information. Specific consideration should be given to the siting of devices on which confidential or sensitive information is processed or retrieved;
  - equipment is sited to avoid environmental damage from causes such as dust & heat;
  - users have been instructed to avoid leaving computers logged-on when unattended if unauthorised access to the data held can be gained. Clear written instructions to this effect should be given to users;
  - users have been instructed not to leave hard copies of sensitive data unattended on desks.
- The same rules apply when accessing the School's ICT System or ICT data away from school, e.g. at a User's home or visiting another school.

6.3. Inventory

- The Headteacher, in accordance with the School's Financial Regulations, shall ensure that an inventory of all ICT equipment is maintained and all items accounted for at least annually.

7. Legitimate Use

7.1. The school's ICT facilities must not be used in any way that breaks the law or breaches Council standards.

7.2. Such breaches include, but are not limited to:

- making, distributing or using unlicensed software or data;
- making or sending threatening, offensive, or harassing messages;
- creating, possessing or distributing obscene material;
- unauthorised personal use of the school's computer facilities.

7.3. Private Hardware & Software

- Dangers can occur from the use of unlicensed software and software infected with a computer virus. It is therefore vital that any private software permitted to be used on the school's equipment is acquired from a responsible source and is used strictly in accordance with the terms of the licence. The use of all private hardware for school purposes must be approved and recorded by the Network/System Manager.

7.4. ICT Security Facilities

- The school's ICT systems and data will be protected using appropriate security arrangements outlined in the rest of Section 7. In addition consideration should also be given to including appropriate processing controls such as audit trails, input validation checks, control totals for output, reports on attempted unauthorised access, etc.

- For new systems, it is recommended that such facilities be confirmed at the time of installing the system. Information on the range of such facilities can be sought from the Council's ICT Services Team.

7.5. Authorisation

- Only persons authorised in writing by the System Manager, are allowed to use the school's ICT systems. Written authorisation outlines the extent to which an ICT User may make use of the ICT System.
- Failure to establish the limits of any authorisation may result in the school being unable to use the sanctions of the Computer Misuse Act 1990. Not only will it be difficult to demonstrate that a user has exceeded the authority given, it will also be difficult to show definitively who is authorised to use a computer system.
- Where ICT systems are available for use, messages should be displayed to users warning against unauthorised use of the system. This may take the form of warnings displayed by the ICT system itself, the use of wall displays or other display suitable to that environment.
- Access eligibility will be reviewed continually, including remote access for support. In particular the relevant access capability will be removed when a person leaves the employment of the school. In addition, access codes, user identification codes and authorisation rules will be reviewed whenever a user changes duties.
- Failure to change access eligibility and passwords will leave the ICT systems vulnerable to misuse.

7.6. Passwords

- The level of password control will be defined by the System Manager based on the value and sensitivity of the data involved, including the possible use of "time out" passwords where a terminal/PC is left unused for a defined period.
- Passwords for staff users should be changed regularly and should not be re-used. They should be a minimum of 8 characters, including a mix of letters and numbers.
- Passwords should be memorised and not written down.
- Passwords or screen saver protection should protect access to all ICT systems. The BIOS (the first code run by a PC when powered on) area of ICT devices should be protected with a password to restrict unauthorised access.
- A password must be changed if it is affected by a suspected or actual breach of security or if there is a possibility that such a breach could occur, such as:
    - when a password holder leaves the school or is transferred to another post;
    - when a password may have become known to a person not entitled to know it.
- The need to change one or more passwords will be determined by the risk of the security breach.
- Users must not reveal their password to anyone. Users who forget their password must request the System Manager issue a new password.

7.7. Encryption

- As a minimum, all devices of the ICT System that are portable should be fully encrypted to meet the current standards outlined by Becta (see http://www.tamesideschoolssupport.net for further information). Devices subject to encryption may include:
    - Laptops
    - PDAs
    - Smartphones/Blackberries
    - USB Pendrives/Memory cards
- Where technology prevents the use of encryption (e.g. SD Memory Cards used in Digital Cameras) then any data deemed Impact Level 2 or above should not be stored on these devices.
- When using encryption systems that require a password to access the system, the same guidance for passwords outlined in Section 7.6 applies.

7.8. Filtering of the Internet

- Access to the internet for children should be filtered using an approved system. In Tameside MBC all schools connected through the Wide Area Network have their internet filtered using a Becta accredited filtering solution (see http://www.tamesideschoolssupport.net for current details).
- It is the responsibility of the ICT System Manager to monitor the effectiveness of filtering at the school and report issues to Tameside MBC.
- Where breaches of internet filtering have occurred, the ICT System Manager should inform the Headteacher and assess the risk of continued access.

7.9. Backups

- In order to ensure that essential services and facilities are restored as quickly as possible following an ICT system failure, back-up copies of stored data will be taken at regular intervals as determined by the System Manager, dependent upon the importance and quantity of the data concerned.
- Where programs and data are held on the Council's systems or other multi-user system, data security and restoration is covered by Tameside MBC procedures.
- Data essential for the day to day running and management of the school should be stored on the school's network.
- Backups contain data that must be protected and should be clearly marked as to what they are and when they were taken. They should be stored away from the system to which they relate in a restricted access fireproof location, preferably off site.
- Instructions for re-installing data or files from backup should be fully documented and security copies should be regularly tested to ensure that they enable the systems/relevant file to be re-loaded in cases of system failure.

7.10. Operating System Patching

- The Network/System manager will ensure that all machines defined as part of the ICT System are patched up to date according to those releases distributed by the manufacturers of the operating systems. A record should be maintained of all machines running operating systems that can be patched along with each machine's patch status.

7.11. Virus Protection

- The school will use appropriate Anti-virus software for all school ICT systems.
- All Users should take precautions to avoid malicious software that may destroy or corrupt data.
- Teachers who have laptops which are taken away from school and may spend periods of days and/or weeks disconnected from the school's network, must take the necessary steps to ensure anti-virus protection software on their laptop is updated as soon as possible after a period of time off the network. The ICT system Manager will have a documented procedure to explain this.
- The school will ensure that every ICT user is aware that any device in the ICT system (PC, laptops, netbook, PDA, cashtill) with a suspected or actual computer virus infection must be disconnected from the network and be reported immediately to the System Manager who must take appropriate action, including removing the source of infection.
- The governing body could be open to a legal action for negligence should a person suffer as a consequence of a computer virus on school equipment.
- The school's internet link is provided by Tameside MBC, procured through a 3rd party. The terms of this connection retain a sanction to remove the connection from the whole Tameside estate if significant viral activity is detected by that 3rd party provider. As such, the school will be notified by Tameside MBC if this is where the viral activity arises from. The ICT System Manager is responsible for the treatment of any virus problems within an agreed period from notification by Tameside MBC. The authority reserves the right to

disconnect a school that fails to comply with a notification order to protect the access for all other schools.

- Any third-party laptops not normally connected to the school network must be checked by the System manager for viruses and anti-virus software before being allowed to connect to the network.
- The school will ensure that up-to-date anti-virus signatures are applied to all servers and that they are available for users to apply, or are automatically applied, to PCs or laptops.

7.12. Disposal of Waste

- Disposal of waste ICT media such as print-outs, floppy diskettes and magnetic tape will be made with due regard to the sensitivity of the information they contain. For example, paper will be shredded if any confidential information from it could be derived.
- The Data Protection Act requires that adequate mechanisms be used when disposing of personal data.

7.13. Disposal of Equipment

- The Data Protection Act requires that any personal data held on a part of the ICT system subject to disposal to be destroyed.
- Prior to the transfer or disposal of any ICT equipment the ICT System Manager must ensure that any personal data or software is obliterated from the machine if the recipient organisation is not authorised to receive the data. Where the recipient organisation is authorised to receive the data, they must be made aware of the existence of any personal data to enable the requirements of the Data Protection Act to be met. Normal write-off rules as stated in Financial Regulations apply. Any ICT equipment must be disposed of in accordance with WEEE regulations.
- It is important to ensure that any copies of the software remaining on a machine being relinquished are legitimate. Care should be taken to avoid infringing software and data copyright and licensing restrictions by supplying unlicensed copies of software inadvertently. The school should maintain a regularly updated asset register of licenses and should indicate when licenses have been transferred from one part of the ICT system to another.

7.14. Repair of Equipment

- If a machine, or its permanent storage (usually a disk drive), is required to be repaired by a third party the significance of any data held must be considered. If data is particularly sensitive it must be removed from hard disks and stored on floppy disk or other media for subsequent reinstallation, if possible. The school will ensure that third parties are currently registered under the Data Protection Act as personnel authorised to see data and as such are bound by the same rules as school staff in relation to not divulging the data or making any unauthorised use of it.

8. Security Incidents

8.1. All suspected or actual breaches of ICT security shall be reported to the System Manager or the Headteacher in their absence, who should ensure a speedy and effective response to be made to an ICT security incident, including securing useable evidence of breaches and evidence of any weakness in existing security arrangements. They must also establish the operational or financial requirements to restore the ICT service quickly.

8.2. The Audit Commission's Survey of Computer Fraud and Abuse 1990 revealed that over 50% of incidents of ICT misuse are uncovered accidentally. It is, therefore, important that users are given positive encouragement to be vigilant towards any suspicious event relating to ICT use.

8.3. It should be recognised that the school and its officers may be open to a legal action for negligence if a person or organisation should suffer as a consequence of a breach of ICT security within the school where insufficient action had been taken to resolve the breach.

9. Acceptable Use Policy

9.1. The school's Acceptable Use Policy applies to all school staff, students and third parties who use either or both of these facilities. The policy covers the use of hardware supplied by the school, email, the Internet, services accessed through the Internet and local file and network usage. The conditions of use are explained in the policy. All school staff accessing these facilities must be issued with a copy of the 'Acceptable Use Policy and other relevant documents and complete the user declaration attached to the policy. For all students, the school will ensure that the relevant 'Acceptable Use Policy' document is issued and the consent form is completed by pupils and their parents. In addition, copies of the 'Acceptable Use Policy' document and consent form will be issued to all visitors.

10. Personal Use

10.1. The School has devoted time and effort into developing the ICT Systems to assist you with your work. It is, however, recognised that there are times when you may want to use the Systems for non-work related purposes, and in recognising this need the School permits you to use the Systems for personal use, so long as this use is not considered to be 'significant'.

- *NB: in this school 'significant' is defined as interfering with contracted time that would otherwise be spent on work. So, for example, if a staff member used a laptop to access personal emails during specified work time, this would be seen as a contravention. However, if the staff member chose to take the laptop home and, in the course of continuing school work, chose to access personal emails, this would not be seen as a contravention.*

10.2. You must not use the systems for personal use during directed working hours. You must not allow personal use of systems to interfere with your day to day duties. Any non-job related use of the systems during working hours may be subject to disciplinary action.

10.3. You must not use School software for personal use unless the terms of the licence permit this and you are responsible for checking the licensing position. Microsoft Office and Internet Explorer are licensed for personal use.

10.4. Use of the systems should at all times be strictly in accordance with the provisions of paragraph 9.1 above. You must pay all costs associated with personal use at the School's current rates e.g. cost of paper.

10.5. You are responsible for any non business related file which is stored on your computer.

10.6. When accessing the internet for non work purposes you may only view web pages and download .pdf files.

11. Disciplinary Implications

11.1. Breaches of this policy may result in disciplinary action up to and including dismissal. They may also result in you being prosecuted under the Computer Misuse Act 1990, and may lead to prosecution of the School and the individual(s) concerned and/or civil claims for damages.

E -Safety Policy

POLICY FOR INTERNET ACCESS

Document Purpose
This policy reflects the values and philosophy of Poplar Street in relation to the teaching, learning and guidance of IT systems, electronic IT devices and internet access.

All pupil and staff activity, when using the network and Internet in school, must be in support of education or research and must be appropriate to the educational objectives of the school. Pupils who access the Internet from the school site are responsible for everything that takes place on their computers and all internet activity is logged. Staff use of the internet systems is governed in the document above.

Benefits
Access to e-mail and the Internet will enable staff and the pupils to:

- Explore thousands of libraries, databases, museums and other repositories of information;
- Exchange personal communication with Internet users around the world;
- To link with European and Non European schools through the use of faxes, e-mail and video conferencing;
- Be included in Government initiatives and global educational projects;
- Keep abreast of news and current events;
- Take part in discussions with experts;
- Publish and display work by creating personal web pages.

Safety
Internet access at Poplar Street is provided through the LEA using fast broadband technology and a machine is dedicated to serving the Internet provision directly to the school network. This machine is protected by a secure filing system (Cyber Patrol) which operates to block access to inappropriate materials. All web activity is logged so that pupil's activity can be monitored.

Personal Security Guidelines

- Never reveal personal information, either their own or others, such as home addresses, telephone numbers and Email addresses.
- Do not use photographs of themselves on their web pages unless the parent or guardian has given permission to do so

Mobile Phone Use

- Staff must have their phones on 'silent' or switched off during class time.
- Staff may not make or receive calls during teaching time. If there are extreme circumstances (eg. acutely sick relative) the member of staff will have made the HT aware of this and can have their phone in case of having to receive an emergency call.
- Use of phones must be limited to non-contact time when no children are present.
- Phones must be kept out of sight (eg. handbag, pocket) when staff are with children.
- Calls/ texts /other use must be made/ received in private during non-contact time.
- Phones will never be used to take photographs of children or to store personal data.
- A school mobile will be carried to sporting fixtures away from school or on an educational visit for contacting parents in the event of an emergency.
- For pupils required to bring mobile phones, a letter must be provided by parents/carers giving consent. They must be left at the school office, switched off.

Effective Use and Expectations of Pupils Using the Internet

Internet access will be planned to enrich and extend learning activities as an integral aspect of the curriculum.

Pupils will:

- Be expected to read and agree the Internet agreement;
- Be responsible for their own behaviour on the Internet. This includes materials they choose to access and any language they use;
- When using the World Wide Web be expected not to deliberately seek out offensive materials. Should any pupils encounter any such material accidentally, they are expected to report it immediately to a teacher;
- Ask permission from a member of staff before using the Internet;
- Understand that the school may check their computer files and may monitor the Internet sites, which they visit,
- Know not to complete and send forms without permission from a teacher;
- Know not to give their full name, home address, or telephone number when completing forms;
- Ask permission from a teacher before checking the e-mail;
- Immediately report any unpleasant messages sent to them because this would help protect other pupils and themselves;
- Understand that e-mail messages they receive or send may be read by others;
- Only send messages which are polite and responsible;
- Only send e-mails to people they know or a person their teacher has approved;
- Only send an e-mail when it has been checked by their teacher;
- Not use e-mail to arrange to meet someone outside school hours.

Using the Internet to enhance learning

Pupils will learn how to use a web browser. Older pupils will be taught to use suitable web search engines. Staff and pupils will begin to use the Internet to find and evaluate information. Access to the Internet will become a planned part of the curriculum that will enrich and extend learning.

As in other areas of their work, we recognize that pupils learn most effectively when they are given clear objectives for Internet use.

Different ways of accessing information from the Internet will be used depending upon the nature of the material being accessed and the age of the pupils:

- Access to the internet may be by teacher (or sometimes other adult) demonstration;
- Pupils may access teacher prepared materials, rather than the open internet;
- Pupils may be given a suitable web page or a single web site to access;
- Pupils may be provided with lists of relevant and suitable web sites which they may access;
- Older, more experienced, pupils may be allowed to undertake their own Internet search. Pupils will be expected to observe the Rules of Responsible Internet use and will be informed that checks can and will be made on files held on the system and the sites they access.

Pupils accessing the Internet will be supervised by an adult, normally their teacher, at all times. They will only be allowed to use the Internet once they have been taught the Rules of Responsible Internet Use and the reasons for these rules. Teachers will endeavour to ensure that these rules remain uppermost in the children's minds as they monitor the children using the Internet.

Using Information from the Internet

We believe that, in order to use information from the Internet effectively, it is important for pupils to develop an understanding of the nature of the Internet and the information available on it. In particular, they should know that, unlike the school library for example, most of the information on the Internet is intended for an adult audience, much of the information on the Internet is not properly edited and most of it is copyright.

- Pupils will be taught to expect a wider range of content, both in level and in audience, than is found in the school library or on TV;
- Teachers will ensure that pupils are aware of the need to validate information whenever possible before accepting it as true, and understand that this is even more important when considering information from the Internet.
- When copying materials from the Web, pupils will be taught to observe copyright;
- Pupils will be made aware that the writer of an e-mail or the author of a web page may not be the person claimed.

Using E-mail

Pupils will learn how to use an e-mail application and be taught e-mail conventions. Staff and pupils will begin to use e–mail to communicate with others, to request information and to share information.

- Pupils will only be allowed to use e-mail once they have been taught the Rules of Responsible Internet Use and the reasons for these rules.

- Teachers will endeavour to ensure that these rules remain uppermost in the children's minds as they monitor children using e-mail;
- Pupils may send e-mail as part of planned lessons but will not be given individual e-mail accounts at present;
- In-coming e-mail to pupils will not be regarded as private; (at present children do not have their own accounts)
- Children will have e-mail messages they compose checked by a member of staff before sending them;
- The forwarding of chain letters will not be permitted;
- Pupils will not be allowed to use e-mail to arrange to meet someone outside school hours.

Web site

Our school web site is intended to:

- Provide accurate, up-to-date information about our school;
- Enable pupils to publish work to a high standard, for a very wide audience including pupils, parents, staff, governors, members of the local community and others,
- Celebrate good work;
- Provide pupils with the opportunity to publish their work on the Internet;
- Promote the school;
- In the future it may be used to publish resources for projects or homework.

The point of contact on the web site will be the school address, telephone number and e-mail address. We do not publish pupils' full names or photographs that identify individuals on our web pages, without prior permission of a parent. Home information or individual e-mail identities will not be published. Staff will be identified by their title and surname unless they request otherwise. Permission will be sought from other individuals before they are referred to by name on any pages we publish on our web site.

E–Safety complaints.

Complaints about Internet misuse will be dealt with under the School's complaints procedure. Any complaint about staff misuse will be referred to the head teacher.

All e–Safety complaints and incidents will be recorded by the school, including any actions taken. Pupils and parents will be informed of the complaints procedure. Parents and pupils will need to work in partnership with the school to resolve issues. All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns. Discussions will be held with the local Children's Safeguard Team and local police representatives to establish procedures for handling potentially illegal issues. Any issues (including sanctions) will be dealt with according to the school's disciplinary, behaviour and child protection procedures.

All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.

Internet use across the community

The school will liaise with local organisations to establish a common approach to e–Safety. The school will be sensitive to Internet-related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice. The school will provide appropriate levels of supervision for students who use the internet and technology whilst on the school site. The school will provide an AUP for any guest who needs to access the school computer system or internet on site.

Cyberbullying

Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour. Within the School's behaviour and anti-bullying policy there are clear procedures in place to support anyone in the school community affected by bullying. For cyberbullying these systems may also include the following:

- All incidents of cyberbullying reported to the school will be recorded.
- There will be clear procedures in place to investigate incidents or allegations of Cyberbullying (see behaviour policy)
- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify the perpetrator, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the school's e-Safety ethos.

Sanctions for those involved in cyberbullying may include:

- The perpetrator will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content.
- Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour policy or Acceptable Use Policy.
- Parent/carers of pupils will be informed.
- The Police will be contacted if a criminal offence is suspected.

Staff Agreement:

I agree to abide by the terms and conditions of these policies. I understand that it is my responsibility to ensure the safety and security of all IT equipment supplied to me as part of my role in school.

I understand the need to support and develop my own and children's awareness of e-safety issues and use IT, including the use of the internet and any software appropriately.

I understand the need to protect data, including the use of encryption of all devices if data is removed from school.

Signed…… date……..