Palatine Primary School

ICT Strategic & Operational Policy

WSCC Model Policy September 2012

Reviewed: August 2016

Ratified by the Management Committee: September 16

Date of next Review: August 2019

Contents:

1: Acceptable Use Policy

Networked resources, including Internet access, are potentially available to students and staff in the school. All staff are required to follow the conditions laid down in this policy. Any breach of these conditions may lead to withdrawal of the user's access; monitoring and or retrospective investigation of the users use of services, and in some instances could lead to criminal prosecution. Any breach of the conditions will also be considered a disciplinary matter.

Networked resources are intended for educational purposes, including administrative work, and may only be used for legal activities consistent with the rules of Palatine Primary School. Any expression of a personal view about the school or County Council matters in any electronic form of communication must be endorsed to that effect. Any use of the network that would bring the name of the school or County Council into disrepute is not allowed.

Palatine Primary School expects that staff will use new technologies as appropriate within the curriculum and that staff will provide guidance and instruction to pupils in the use of such resources.

Unsupervised pupil use of the Internet or Palatine Primary school's Intranet is not allowed

All computer systems will be regularly monitored to ensure that they are being used in a responsible fashion.

Conditions of Use

Personal Responsibility

Access to the networked resources is a privilege, not a right. Users are responsible for their behaviour and communications. Staff, and pupils, will be expected to use the resources for the purposes for which they are made available. Users are to take due care with the physical security of hardware they are using. Users will accept personal responsibility for reporting any misuse of the network to the ICT Coordinator/s and / or senior management.

Concerns of a child protection nature must be referred to the Senior Designated Professional for Safeguarding and dealt with in accordance with school child protection procedures.

Acceptable Use

Users are expected to utilise the network systems in a responsible manner.

Network Etiquette and Privacy

Users are expected to abide by the rules of network etiquette. These rules include, but are not limited to, the following:

1. Be polite – never send or encourage others to send abusive messages.

2. Use appropriate language – users should remember that they are representatives of the school on a global public system. Illegal activities of any kind are strictly forbidden.

3. Do not use language that could be calculated to incite hatred against any ethnic, religious or other minority group.

4. Privacy – do not reveal any personal information (e.g. home address, telephone number) about yourself or other users. Do not trespass into other user's files or folders.

5. Password – do not reveal your password to anyone. If you think someone has learned your password then contact the ICT coordinator / senior management.

6. Electronic mail – Is not guaranteed to be private. Messages relating to or in support of illegal activities will be reported to the authorities. Do not send anonymous messages.

7. Disruptions – do not use the network in any way that would disrupt use of the network by others.

8. Pupils will not be allowed access to unsupervised and/or unauthorised chat rooms and should not attempt to gain access to them.

9. Staff or students finding unsuitable websites through the school network should report the web address to the ICT coordinator / senior management.

10. Do not introduce “pen drives” into the network without having them checked for viruses.

11. Do not attempt to visit websites that might be considered inappropriate. (Such sites would include those relating to illegal activity; all sites visited leave evidence in the county network if not on the computer. Downloading some material is illegal and the police or other authorities may be called to investigate such use.

12. Unapproved system utilities and executable files will not be allowed in pupils’ work areas or attached to e-mail.

13. Files held on the school’s network will be regularly checked by ICT coordinator / ICT technician.

14. It is the responsibility of the User (where appropriate) to take all reasonable steps to ensure compliance with the conditions set out in this Policy document, and to ensure that unacceptable use of the Internet/Intranet does not occur.

Physical security

Staff users are expected to ensure that portable ICT equipment such as laptops, digital still and video cameras are securely locked away when they are not being used.

Wilful damage

Any malicious attempt to harm or destroy any equipment or data of another user or network connected to the school system will result in loss of access, disciplinary action and, if appropriate, legal referral. This includes the creation or uploading of computer viruses. The use of software from unauthorised sources is prohibited.

Unacceptable Use:

- Users must login with their own user ID and password, where applicable, and must not share this information with other users. They must also log off after their session has finished.

- Users finding machines logged on under other users username should log off the machine whether they intend to use it or not.

- Accessing or creating, transmitting, displaying or publishing any material (e.g. images, sounds or data) that is likely to cause offence, inconvenience or needless anxiety.

- Accessing or creating, transmitting or publishing any defamatory material.

- Receiving, sending or publishing material that violates **copyright** law. This includes through Video Conferencing and Web Broadcasting

- Receiving, sending or publishing material that violates **Data Protection Act** or breaching the security this act requires for personal data.

- Transmitting unsolicited material to other users (including those on other networks).
- Unauthorised access to data and resources on the school network system or other systems.

- User action that would cause corruption or destruction of other users' data, or violate the privacy of other users, or intentionally waste time or resources on the network or elsewhere.

- Keeping confidential information in an open file on the school network is not allowed.

2: Misuse of the Internet

Misuse of the Internet service provided by the School includes but is not limited to:

- Searching for or making, sending, displaying or publishing any material (e.g. imagery, sound or information) that is likely to cause offence, inconvenience, needless anxiety and/or bring the school into disrepute.
- Searching for / looking at, making or publishing offensive material.
- Receiving, publishing or sending material that breaks Copyright Law or the Data Protection Act.
- Sending unsolicited material to other users (including those on other networks)
- Trying to look at data and resources on the school office network system or other systems outside school unless permission has been granted.
- Acting in a way that would cause corruption or destruction of other users' data, violate the privacy of other users or intentionally waste time or resources on the school system or elsewhere.
- Downloading software without the approval of the *member of staff responsible*.
- Spending excessive amounts of time using the Internet for non-school/work related reasons. (Incidental personal use is permitted provided it complies with these protocols and does not interfere with work or study).

Failure to adhere to these protocols may result in loss of access to the Internet as well as other disciplinary action.

Other Considerations

- Being polite and never sending, or encouraging others to send, abusive messages. Defamatory comments could result in legal action. E-mail has been used successfully as evidence in libel cases.
- Using appropriate language. Users should remember that they are representatives of the school on a global public system. Illegal activities of any kind are strictly forbidden.
- E-mail is not guaranteed to be private. Messages relating to or in support of illegal activities will be reported to the authorities. Anonymous messages should not be sent. The school reserves the right to apply monitoring arrangements in relation to e-mail use where misuse is suspected.

- Not using the Internet in any way that would disrupt the use of the network by others. The school reserves the right to apply monitoring arrangements to any student or member of staff in relation to Internet use and related services where misuse is suspected.

The Purpose of Monitoring or the Investigation of Users

- To ensure compliance with the schools Acceptable Use Policy
- To investigate unauthorised use of the Internet and e-mail systems.
- To protect the operational availability and performance of ICT technical infrastructure.
- To continue the work of a school if an addressee is absent.
- To comply with the County Council's statutory obligations.
- To prevent or detect crime.

Filtering

In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor West Sussex County Council can accept liability for the material accessed, or any consequences of Internet access. Palatine Primary School must gain parental permission before pupils are able to access the Internet.

Despite careful design, filtering systems cannot be completely effective due to the speed of change of Internet content. Filtering may be performed by:

- Internet Service Provider
- School-level systems (Smoothwall) or
- any combination of the above

Careful monitoring and management of all filtering systems is carried out by the ICT Technician

Action for Schools - Filtering

- The school will work in partnership with parents, the local authority, DfES and the Internet Service Provider to ensure that the Internet filter systems protect pupils and are reviewed and improved.
- If staff or pupils discover unsuitable sites, the URL (website address) and content must be reported to the Internet Service Provider via the nominated contact / ICT Coordinator
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Headteachers having reasonable suspicion that a member of staff is misusing the system may consult with their HR Business Partner to obtain guidance before instigating an investigation into e-mail or Internet Access misuse.

3: Email Protocols

Palatine Primary School reminds pupils (where appropriate), and staff that the Office 365 e-mail service must be used in an appropriate manner. Staff of Palatine Primary School should be aware of the following bullet point list that shows some of the key principles of e-mail use.

- All users need to follow the guidelines set out in the Network etiquette section of this document.
- Pupils (where able), and staff may only use approved e-mail accounts on the school system.
- E-mail is not guaranteed to be private. Any suspected unauthorised use of the email system will be investigated to ensure compliance with these Protocols. Messages relating to or in support of illegal activities will be reported to the authorities.
- Anonymous messages should not be sent.
- Messages that are likely to bring the school into disrepute should not be sent.
- Staff (and pupils where able), must immediately inform the ICT Technician / Coordinator if they receive offensive e-mail.
- No person using the email service should reveal details of themselves or others in e mail communication, such as address or telephone number, or arrange to meet anyone.
- Access in school to external personal e-mail accounts may be blocked.
- Excessive social e-mail use can interfere with learning and may be restricted. (Incidental personal use is permitted provided it complies with these protocols and does not interfere with work or study).
- The forwarding of chain letters is not permitted.
- E-mail sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper.
- Do not open suspect emails or attachments; it may contain a virus.

Staff should also be aware that e-mail is not a secure medium and should not normally be used for sensitive or confidential information.

4: Use of Digital Images

There are many circumstances where schools may wish to publish digital images (either video or still) of students or their work. Care needs to be taken when placing any of this material into the public domain.

For the purposes of this section publication includes on websites, in the press, on TV, as web broadcasts or video/CVD/DVD to be released into the public domain.

Palatine Primary School will:

- Gain written permission from parents or carers before photographs of pupils are published on the school web site/Zaptap communication App/Smart screens.
- Named images of pupils must not be published in any circumstance. This includes photographs, videos, TV presentations, web pages, the press etc.
- The head teacher or Business Manager will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The school web site should comply with the school's guidelines for publications.
- Pupils' work will only be published (e.g. photographs, videos, TV presentations, web pages, press etc) if parental consent has been given. A Photographer / Videographer Consent Form can be found in chapter 14 of this document.

The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

5: Video Conferencing

Video Conferencing (VC) provides users with access to high quality video conferencing, and the ability to use file share, chat, and whiteboard functions. Conferencing can be on a one to one basis, or a multi-conference involving many individuals or groups. VC is provided for educational use to improve communications and school curriculum activities.

Action for Schools

- Care should be taken to ensure copyright law is adhered to where appropriate.
- Any license conditions related to the commercial use of software available over the Internet must be observed.
- Responsibility for security lies with all users - any abnormal or unexpected occurrence while using the service must be immediately reported to ICT coordinator / senior management.
- Apply the guidelines set out in Network etiquette to the use of VC

The following are not permitted:

- disrupting a service
- accessing sites which have been expressly prohibited
- downloading inappropriate information
- disclosure of confidential information
- the use of profanities
- any malicious or illegal use of the service

6: Web Broadcasting

Web broadcasting includes web presentation, Blogging, audioblogging, Moblogging and vlogging, mobcasting, posting and streaming audio and video to the Internet. Schools wishing to implement web broadcasting in some form will need to take the following into consideration:

- Web broadcasting is at the schools discretion and risk. The school will be solely responsible for any damages to the computer system or loss of data resulting from the download of such material or data.
- Users must respect the legal protection provided by copyright and license to musical content, programs and Data.
- Malicious use is not acceptable.
- Consideration to be given of how content will be available, either by streaming or download.
- Avoid referring to children by name when filming, or use a sound effect to ‘bleep’ it out of the web version.
- Use character names rather than real names if possible.
- In credits, consider using the teachers name only as a contact. Alternatively, refer to the video as a class project, for example ‘This video was produced by Class 4’.
- Use only pupil first names in any credits, and will not attribute individuals to specific roles. Alternatively, they may consider using two versions of film with different credits – one with full credits for internal school use, and one without credits for external activities such as publishing on the school website or showing at parents’ evenings.

Palatine Primary School will give consideration to the way in which video clips are made available on their website:

- If hosted on a web server, video clips may be downloaded and saved to the viewers' desktop. *Once downloaded, the school has no control over the way in which the video is viewed, edited or distributed.*
- Streamed video can only be viewed and not downloaded (although if a user has sufficient technological understanding and determination, the data can still be captured). Typically, streams can be logged and monitored, including details such as IP address, when and how long the viewer has watched the video. These logs can indicate whether a particular user is showing 'too much' interest in school videos.

8: Copyright

Copyright protection exists to prevent people copying original works without the consent of the author. This includes videos, photos, music and documents.

What is Copyright?
Copyright is part of the family of intellectual property rights (IPR). Copyright aims to protect original work from being copied without permission of its maker. Unlike other IPRs, which must be registered or declared by the creator, copyright exists as soon as the work has been created. Copyright does not protect ideas or facts. It protects the way the facts or ideas have been recorded.

Generally, the creator/author or the company they work for owns copyright. Only they can give permission for others to use it.

Current UK copyright legislation is based on the Copyright, Designs and Patents Act 1988, but is also supplemented by various European Commission Directives.

Copyright also applies to databases - it is called Database Right. Like Copyright it is an automatic right. Database Right only lasts for 15 years, but may be extended if the databases changes significantly and it covers the extraction and reutilisation of the contents of a database. Examples of databases include encyclopaedias, dictionaries, online collections as well as WebPages and other collections of data on the Internet.

The Law
The infringement of copyright is a criminal offence under the Copyright, Designs and Patents Act 1988 and could result in prosecution. In addition, copyright owners have the right to seek damages from a breach or to obtain an injunction to prevent one

8: Data Protection

Schools hold information on both pupils and staff and in doing so, must follow the requirements of the 1998 Data Protection Act (DPA). The DPA covers the collection, storing, editing, retrieving, disclosure, archiving and destruction of personal data. The Act now applies to data held on paper as well as electronically. For example - it applies to teacher records/mark books.

Palatine Primary School is registered with the Information Commissioner.

The DPA contains eight enforceable principles that must be adhered to regarding personal data as well as a number of conditions that apply.

Personal Data is data that relates to a living individual who can be identified from that data or that data and other data held by the data controller, i.e. the School.

All Personal Data held must be:

1. Fairly and lawfully processed
2. Processed for limited purposes
3. Adequate, relevant and not excessive
4. Accurate
5. Not kept longer than necessary
6. Processed in accordance with the data subject's rights
7. Secure; only available to those with necessary need
8. Not transferred to countries without adequate protection.

9: Enforceable Principles

Principle 1. *Personal Data must be fairly and lawfully processed.*
Persons in schools that are collecting data need to clearly and accurately inform those who are providing data how that data is going to be used. Under most circumstances the data will be held for “normal administrative education purposes”. Consent will only be valid if fair processing information has been given. Ideally, consent recorded in writing is the most appropriate.

Palatine Primary School, after collection, may decide it would like to use all or part of the data for other purposes, beyond the scope of the original declared purpose. If this occurs the school must inform the parent, pupil (if appropriate) or member of staff of the proposed use and give them the opportunity to object to the use if they wish.

Principle 3. *Data held should be adequate, relevant and not excessive.*
Schools holding any data on individual staff or students must ensure that, if challenged, can provide good reasons for the need to hold it.

Principle 5. *Data should not be kept longer than necessary.*
Any data held by the school should not be retained for longer than is necessary for the purpose declared to the member of staff or student concerned. An appropriate review procedure should therefore be adopted to ensure that data is destroyed when it is no longer required. (Legally prescribed retention periods may apply in some cases for example pupil records should be retained until the pupil is 25 years old).

Principle 7. *Data should be kept Secure.*
The type of security measures that a school should take to protect personal information from

unauthorised use or accidental damage should reflect the harm that would result from a failure to protect it.

Under the Data Protection Act (DPA) - “An individual can claim compensation from a data controller (school) for damage and distress caused by any breach of the act”.

Pupils (where appropriate), staff and parents have the right to see their Personal Data held by the school.

Under these regulations, the governing body of a school must make a **pupil’s educational record** available for inspection by the parent, free of charge, within 15 school days of the parent’s written request for access to that record.

The school must also provide a copy of the record if requested to do so in writing within 15 school days. The school may charge a fee not exceeding the cost of supply.

Registration
Under the DPA, each school must notify details about its processing of Personal Data to the Information Commissioner. The fee for notification is now £35 for one year. The governing body or head teacher will receive the appropriate forms prior to the expiry of their registered entry. An application for notification can be made either via the Commissioner's website, or by telephoning the Notification Department (01625 5457400).

10: Health and Safety

- There is space at the computers for children and staff to comfortably work.
- Health and safety regulations are adhered to. For example, children or staff working on extended activities are encouraged to have a ten minute break from the computer in every hour
- Monitors are positioned properly, e.g. glare and strain are reduced.
- ‘Touch-screens’ are easily reached.
- Pupils and staff are encouraged not to stare into the beam from projectors
- The data projector light is positioned properly in those classes that do not have a Clevertouch screen installed
- The interactive whiteboard is non-reflective so as to reduce glare.
- Blinds fitted at windows, where appropriate.
- The chairs at the computers are of the correct size for the children and staff
- Desks or benching are at the correct height (or are adjustable).
- Physical well-being can be promoted by the use of devices in open spaces, where possible, and that are suited to individual needs.
- Mental well-being is promoted by learning activities which promote challenge, allow achievement and which are enjoyable.
- A personalisation agenda has been adopted, meaning that each child has choice, which helps to promote mental well-being.
- There are no trailing wires in places where electrical equipment is used
- Pupils do not use electrical equipment unsupervised
- Electric sockets and equipment are positioned away from water sources.

11: Network Security

Users are expected to employ good password practice when using the network. This includes keeping personal passwords secure and always logging off after use.

Users are also expected to inform *member of staff responsible* immediately if a security problem is identified. Do not demonstrate this problem to other users. Users must login with their own user id and password, where applicable, and must not share this information with other users. Users identified as a security risk will be denied access to the network.

The Network Manager ensures that:

- The server operating system must be secured to a high level.
- User's desktops are "locked down" sufficiently to prevent casual / accidental damage by users.
- Staff are not allowed to keep confidential files on the open network.
- Anti Virus software (Eset) is both installed throughout the network and kept up to date. This includes taking steps to allow staff laptops to receive updates either at home or in school.
- Steps are taken to ensure that Windows critical updates are both downloaded and installed on a regular basis.
- All Internet connections must be assessed for security risks including the wide area network connection and any modems staff may wish to use.
- Wireless networks use at least WEP (Wired Equivalent Privacy) encryption to prevent unauthorised access to their network.

12: Hardware Security

PALATINE PRIMARY SCHOOL:

- Ensures that all costly ICT equipment is boldly security marked in a high visibility area on the device and serial numbers are inventoried. Major items of equipment may also need to secured using cages, alarms or other security measures as appropriate.
- The Network Manager ensures that network servers are located securely and physical access restricted.
- Staff users must ensure that portable ICT equipment such as laptops, Ipads, digital still and video cameras are securely locked away when they are not being used.
- Users identified as a security risk may be denied access to these types of equipment.

Guidance for using iPads more securely.

Apple's iPad is a highly versatile tool in schools that can be used for a wide variety of tasks by staff working with young people in schools. An iPad combines hardware and software security that can transform the device into one that can be more secure than your PC or Mac. However, much of this depends on you taking the right steps to secure it. Making sure you take these steps is particularly important if you use the device to "process" personal or sensitive data for your work in schools.

One of the biggest security risks to data is physically losing your device. This being the case, naturally, the first step is to make sure your iPad is not lost or stolen. Next, and equally important, is ensuring the data held on the iPad is safe in case it is lost or stolen. The techniques to employ here are a combination of: passcodes, encryption and remote wiping.

Keeping your device "healthy"

There are some quite simple steps that can be taken to help reduce the risk of "data leakage" that mirror those taken on laptops and desktop PC's. These steps include:

- Only installing apps that you are confident are legitimate and secure. Your school may have a policy / list for "approved" Apps.
- Pay attention to what permissions an App requires when installing, you could be giving it access to sensitive data held on your device
- Keeping your Apps up to date
- Being cautious of "Phishing" attempts to steal Google, Apple or Social Media accounts
- Follow safe browsing procedures, just like you would on a computer, to avoid viruses and malware
- Using an anti-virus product

Actions if your iPad is lost or stolen.

- Change your password on any Internet based services that you used the iPad to connect to.
- These services may include, but are not limited to: OneDrive, Dropbox, Google Drive or Amazon.
- Report the loss of the device to your senior management team so they may be able mitigate the risk of personal data being lost.
- Login to the Apple iCloud site and use the "Find My iPhone" function to try and locate your iPad
- If your device appears to be in an unauthorised location and your data is at risk you have the option of using the "Erase iPad" function to ensure safety.
- If your device appears to be in an unauthorised location and it is appropriate, inform the police.

14: Agreements and Permissions

Staff Laptops, Ipads and Computers

PROTOCOL

Information:

Please note that laptops allocated to staff remain the property of the school and must be returned to the school if the member of staff leaves the schools employment.

Insurance:

For laptops and Ipads to be covered automatically under the schools policies at no extra charge, they need to be included on the school's inventory. The standard All Risks insurance policy covers the laptops for theft (where there are signs of forced entry), and accidental or malicious damage. Those Schools who have opted for the additional Buildings and Contents policy will also receive cover for flood/water damage, storm damage etc. All equipment in Schools is automatically covered for fire, lightning and explosion.

Laptops and Ipads are not covered by the school policy:

- Whilst in vehicles,
- Left unattended.
- Left unattended in a locked household over 48 hours.

If stolen or damaged from an employee's/student's home, County would first ask for a claim under the teachers household policy. Claims from the School policy will only be made if this were unsuccessful.

Please note that regardless of the policy a stolen laptop is claimed under, a claim will not be considered unless there are signs of forced entry or assault.

In accordance with Financial Regulations, the equipment must be marked as School property and shall be recorded in the Register of Assets/Inventory Book.

PALATINE PRIMARY SCHOOL accepts no liability for any consequences (including financial or other loss), which may arise through private use of the facilities or equipment provided. You should also note that the security of private information and data is your responsibility. *You are advised that simply deleting files does not permanently remove them from a computer.*

Where access to the Internet is provided, by using an unfiltered Internet service, you should be aware that the Internet contains potentially offensive material. West Sussex Local Authority and PALATINE PRIMARY SCHOOL accepts no liability for any offence, injury or consequences that may result from your use of the Internet and its associated facilities.

Legal Implications:

PALATINE PRIMARY SCHOOL must comply with all UK legislation with respect to the use of ICT.

In using PALATINE PRIMARY SCHOOL facilities and equipment you must comply with the following Acts and may be held personally liable for any breach of current legislation as listed below and any future legislation that may be enacted:

- Data Protection Act 1998
- Copyright Designs and Patents Act 1988
- Computer Misuse Act 1990
- Obscene Publications Act 1959
- Freedom of Information Act 2000

It should be noted that:

- There should be no reason to hold PALATINE PRIMARY SCHOOL information requiring registration under the Data Protection Act on computer equipment provided for your use.

- It is your responsibility to ensure that any personal information held on the computer equipment provided by PALATINE PRIMARY SCHOOL complies with the provisions of the Data Protection legislation.

- The transmission of personal information contained within electronic mail or as an attachment to electronic mail is also subject to the provisions of the Data Protection Act.

- Waste media (e.g. printed reports) must be disposed of with regard to the sensitivity of information concerned and all material making reference to personal data must be disposed of in accordance with policies and procedures.

- If you hold private information that contains personal details there may be a requirement to register that information.

- The use, or possession, of unlicensed copies or "pirated" versions of software is illegal and is expressly prohibited under the Copyright Designs and Patents Act.

- Under the Computer Misuse Act 1990, it is an offence:
  (a) to secure computer access to information, data or material where such access is unauthorised, and
  (b) to secure such access with the intent of the commission of a criminal offence.

- The Act also makes it an offence to make any unauthorised modification to the contents of any computer.

- The Obscene Publications Act 1959 makes it an offence to publish an obscene article. Publishing for the purpose of the Act includes distribution or circulation of the article and, in the case of an article containing or embodying matter to be looked at, showing the article.

- Under the Freedom of Information Act 2000 there is a general right of access to all types of recorded information held by public authorities. This will include all information held on your laptop.

---

1. COMPUTER SECURITY

All media (e.g. memory sticks, CDs) of uncertain or unreliable origin must be checked for viruses before use.

Where a virus is suspected/detected, the matter must be repaired and you must refrain from sending electronic mail and exchanging information via computer media with others. Virus repair must be undertaken only by an IT specialist.

It is your responsibility to ensure that information other than programmes and the operating system held on computer equipment provided by the school is secured (backed-up) on a regular basis.

Where stolen equipment and/or software are recovered; or where it is suspected that equipment or software have been tampered with, they must be tested prior to re-use by an IT specialist.

2. RISK MANAGEMENT AND INSURANCE

As part of the schools' risk management and risk financing arrangements, West Sussex Local Authority maintains insurance on the equipment provided to you, including cover against the perils of theft, accidental damage, malicious damage and fire. Cover for theft is, however, subject to loss arising from forcible entry to or exit from your premises and the standard conditions of cover require that all reasonable care and precaution is taken to try and prevent loss of or damage to the equipment. All computer equipment must be secured from theft or unauthorised use as far as is practical.

If you are moving house you are advised to check that the equipment is covered by your removal company's insurance policy.

Any loss of, or damage to, the equipment should be reported as soon as possible to the Head teacher in the first instance and any criminal damage should be reported to the Police.

3. INTERNET ACCESS AND ELECTRONIC MAIL

You are requested to monitor and manage your electronic mail and calendar on a regular basis, preferably daily. You will be provided with an email address to conduct your normal business.

You are reminded that PALATINE PRIMARY SCHOOL facilities and equipment may only be used for lawful purposes. Viewing or transmission of any material, which may be regarded as offensive or in violation of any UK law or legislation, is not permitted. Such material may include copyright material, material judged to be threatening, pornographic, obscene or sexually explicit and material protected by trade secret.

Sending electronic mail, or attaching a file to an email, constitutes processing of personal data if there is any personal data on a living individual within the electronic mail or the attachment. Such processing can only be undertaken if it is permitted under the school's Data Protection notification.

Electronic mail should not be used for the transmission of sensitive and confidential information.

PROBITY

You are reminded of the fact that you are bound by a Code of Conduct and Practice for schools and that the standards for the regulation of the profession contained within the Code also apply to specific instances, such as the use of the Internet, Intranet or e-mail. You should ensure that your conduct accords with the requirements of the Code.

4. HEALTH AND SAFETY

In the interests of health and safety, you are advised to adhere to the following recommendations for the safe use of personal computer equipment:

- Sit in a chair that gives you good back support to avoid backache;
- Position the screen in front of you to avoid twisting;
- Regularly look away from the screen to reduce eyestrain.

While you have been provided with a “laptop” computer, you should avoid using it on a low table or on your lap as both of these positions will increase strain on your neck and lower back.

If you have any concerns relating to the safe use of your computer equipment, please contact the Health and Safety representative in your school.

5. INDEMNITY

You shall indemnify West Sussex Local Authority and PALATINE PRIMARY SCHOOL against any claims, demands, actions, costs, expenses, losses and damages arising from:

a) any breach by you of any of the conditions of this Protocol;
b) any infringement or alleged infringement of any Intellectual Property Right arising from any use of the equipment in combination with any item not supplied by PALATINE PRIMARY SCHOOL