Thames Primary Academy and Children's Centre

eSafety
and
Data Security

Policies for ICT Acceptable Use

Author:	**Julie Allison and Chris Wolfe**
Date of issue:	**February 2013**
Review date:	**March 2014**

Contents

Introduction

Thames Primary Academy provides education, care and support for pupils and their families within the Blackpool community, through the school, nursery and children's centre. In the 21st Century, Information and Communications Technology (ICT) is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools communities need to build in the use of these technologies in order to arm our young people with the skills necessary to access life-long learning and employment.

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

- Websites
- E-mail, Instant Messaging and chat rooms
- Social Media, including Facebook and Twitter
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality
- Gaming, especially online
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, is not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies and that some have minimum age requirements, usually 13 years.

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

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

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

The eSafety Policy and the Acceptable Use Agreement (for all staff, governors, parents, visitors and pupils) are inclusive of both fixed and mobile internet technologies provided by the Academy (such as PCs, laptops, mobile devices, webcams, whiteboards, voting systems, digital video equipment, etc) and technologies owned by pupils and staff but brought onto Academy premises (such as laptops, mobile phones and other mobile devices).

ICT Security

Computer Viruses

- All files downloaded from the Internet, received via e-mail or on removable media such as a memory stick must be checked for any viruses using Academy provided anti-virus software before being used.
- Never interfere with any anti-virus software installed on Academy ICT equipment that you use.
- If your machine is not routinely connected to the Academy network, you must make provision for regular virus updates through the ICT Support Manager.
- If you suspect there may be a virus on any Academy ICT equipment, stop using the equipment and contact the ICT Support Manager immediately. You will be advised what actions to take and they will be responsible for advising others that need to know.

Managing Passwords

- **Always use your own** personal passwords.
- Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures.
- Staff should change temporary passwords at first logon.
- Change passwords whenever there is any indication of possible system or password compromise.
- Do not record passwords or encryption keys on paper or in an unprotected file.
- **Only disclose your personal password to authorised ICT support staff when necessary, and never to anyone else**. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished.
- **Never tell a child or colleague your password.**
- **If you aware of a breach of security with your password or account inform a member of the SLT or ICT Support Manager immediately.**
- Personal passwords must contain a minimum of six characters and be difficult to guess.
- Passwords should contain a mixture of upper and lowercase letters, numbers and symbols.
- User ID and passwords for staff and pupils who have left the Academy are removed from the system within 48 hrs.

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

Monitoring

Authorised ICT staff may inspect any ICT equipment owned or leased by the Academy at any time without prior notice. If you are in doubt as to whether the individual requesting such access is authorised to do so, please ask for their identification badge and contact a member of the senior leadership team (SLT). Any ICT authorised staff member will be happy to comply with this request.

ICT authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice or image) involving employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain Academy business related information; to confirm or investigate compliance with Academy policies, standards and procedures; to ensure the effective operation of Academy ICT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime.

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

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.
Please note that personal communications using Academy ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

All internet activity is logged by the Academy's internet provider and these logs may be monitored by ICT authorised staff.

Security Breaches

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

Any policy breach is grounds for disciplinary action in accordance with the Academy Disciplinary Procedure.

Policy breaches may also lead to criminal or civil proceedings.

The Information Commissioner's Office (ICO) has powers to issue monetary penalties up to £500,000 for serious breaches of the Data Protection Act.

The data protection powers of the ICO are to:

- Conduct assessments to check organisations are complying with the Act;
- Serve information notices requiring organisations to provide the ICO with specified information within a certain time period;
- Serve enforcement notices and 'stop now' orders where there has been a breach of the Act, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;
- Prosecute those who commit criminal offences under the Act;
- Conduct audits to assess whether organisations processing of personal data follows good practice,
- Report to Parliament on data protection issues of concern.

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the Academy's SLT or eSafety Co-ordinator. Similarly, all security breaches, lost/stolen equipment or data (including remote access Secure ID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the Information Risk Owner, Sandra Wolfe.

e-Mail

The use of e-mail within most schools is an essential means of communication for both staff and pupils. In the context of Thames Primary Academy, e-mail should not be considered private. Educationally, e-mail can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an e-mail in relation to their age and good network etiquette.

Sending e-Mails

- If sending e-mails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, refer to the section **Error! Reference source not found.**.
- Use your own Academy e-mail account so that you are clearly identified as the originator of a message.
- Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate.
- Do not send or forward attachments unnecessarily.
- Whenever possible, send the location path to a shared drive rather than sending attachments
- Academy e-mail is not to be used for personal advertising.

Receiving e-Mails

- Check your e-mail regularly.
- Activate your 'out-of-office' notification when away for extended periods.
- Never open attachments from an untrusted source; Consult the ICT Support Manager first.
- Do not use the e-mail systems to store attachments. Detach and save business related work to an appropriate shared location.
- The automatic forwarding and deletion of e-mails is not allowed.

Managing e-Mail

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

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

- Under no circumstances should staff contact pupils, parents or conduct any Academy business using personal e-mail addresses.

- The Academy requires a standard disclaimer to be attached to all e-mail correspondence, stating that, 'the views expressed are not necessarily those of Thames Primary Academy'. The full wording of the disclaimer will be decided by the SLT but the responsibility for adding this disclaimer lies with the account holder.

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

- Staff sending e-mails to external organisations, when not part of their day to day duties, must cc the Headteacher or their line manager.

- Pupils may only use Academy approved accounts on the Academy system and only under direct teacher supervision for educational purposes.

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

    - Delete all e-mails of short-term value.

    - Organise e-mail into folders and carry out frequent house-keeping on all folders and archives.

- The forwarding of chain letters is not permitted.

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

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

- Staff must inform the eSafety co-ordinator or ICT Support Manager if they receive an offensive e-mail.

- Pupils are introduced to e-mail as part of the ICT Scheme of Work.

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

e-Mailing Personal, Sensitive, Confidential or Classified Information

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

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

eSafety

eSafety Roles and Responsibilities

As eSafety is an important aspect of strategic leadership within the Academy, the Headteacher and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named eSafety co-ordinator in the Academy is *Julie Allison,* who has been designated this role as a member of the senior leadership team. All members of the Academy community have been made aware of who holds this post. It is the role of the eSafety co-ordinator to keep abreast of current eSafety issues and guidance.

SLT and governors are updated by the Headteacher/ eSafety co-ordinator and all governors have an understanding of the issues and strategies at our Academy in relation to local and national guidelines and advice.

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

eSafety in the Curriculum

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

- The Academy has a framework for teaching internet skills.
- The Academy provides opportunities within a range of curriculum areas to teach about eSafety.
- Educating pupils about the online risks that they may encounter outside the Academy is done informally when opportunities arise and as part of the eSafety curriculum.
- Pupils are aware of the relevant legislation when using the internet, such as data protection and intellectual property, which may limit what they want to do but also serves to protect them.
- Pupils are taught about copyright, respecting other people's information, safe use of images and other important areas through discussion, modeling and appropriate activities.
- Pupils are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies.; i.e. parent / carer, teacher / trusted staff member, or organisations such as Cybermentors, Childline or CEOP report abuse button,

Pupils are taught to critically evaluate materials and learn good searching skills through cross -curricular teacher models.

Equal Opportunities

Pupils with Additional Needs

The Academy endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the Academys' eSafety rules.

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

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

eSafety Skills Development for Staff

- Staff receive regular information and training on eSafety and how they can promote the 'Stay Safe' online messages.
- New staff receive information on the Academy's acceptable use policy as part of their induction.
- All staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context of eSafety and know what to do in the event of misuse of technology by any member of the Academy community (see flowcharts in appendices).
- All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas.

Managing the eSafety Messages

- We endeavour to embed eSafety messages across the curriculum whenever the internet and/or related technologies are used.
- The eSafety policy will be introduced to the pupils at the start of each academic year.
- eSafety posters will be prominently displayed.
- The key eSafety advice will be promoted widely through school displays, newsletters, class activities and so on.

Incident Management

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the Academy's IRO or eSafety Co-ordinator. Additionally, all security breaches, lost/stolen equipment or data (including remote access SecureID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the Information Risk Owner.

An incident log will be kept to monitor what is happening and identify trends or specific concerns.

Misuse and Infringements

Complaints

Complaints and/ or issues relating to eSafety should be made to the eSafety co-ordinator or Headteacher. Incidents must be logged and the **Flowcharts for Managing an eSafety Incident** (see appendices) should be followed.

Inappropriate Material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the eSafety co-ordinator
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the eSafety co-ordinator and, depending on the seriousness of the offence, investigation by the Headteacher / Governors. This may result in immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.
  Users are made aware of sanctions relating to the misuse or misconduct.

Internet Access

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

Managing the Internet

- The Academy provides pupils with supervised access to Internet resources (where reasonable) through the Academy's fixed and mobile internet connectivity.
- Staff will preview any recommended sites before use.
- Raw image searches are discouraged when working with pupils.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.
- All users must observe software copyright at all times. It is illegal to copy or distribute Academy software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.

Internet Use

- You must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise the intended restricted audience.
- Do not reveal names of colleagues, pupils, or any persons associated with the Academy, discuss Academy business or other confidential information acquired through your job on any social networking site or other online application.
- On-line gambling or gaming is not allowed.
- Academy internet access is controlled through the Blackpool Council web filtering service.
- Staff and pupils are aware that Academy based email and internet activity can be monitored and explored further if required.
- Only designated staff have access to internet logs.
- The Academy uses management control tools for controlling and monitoring workstations.
- If staff or pupils discover an unsuitable site, the screen must be switched off / closed and the incident reported immediately to the e-safety coordinator or teacher as appropriate.
- Anti-virus protection is installed and kept up-to-date on all Academy machines.

Managing Other Web Technologies

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

- At present, the Academy endeavors to deny access to social networking and online games websites to pupils within Academy premises.
- All pupils are advised to be cautious about the information given by others on such websites, for example users not being who they say they are.
- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such websites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- Pupils are always reminded to avoid giving out personal details on websites which may identify them or where they are (full name, address, mobile/ home phone numbers, Academy details, IM/ e-Mail address, specific hobbies / interests).
- Our pupils are advised to set and maintain their online profiles to maximum privacy and deny access to unknown individuals.
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts and information online.
- Our pupils are asked to report any incidents of Cyberbullying to the Academy.
- Staff may only create blogs, wikis or other online areas in order to communicate with pupils using the Academy learning platform or other systems approved by the Headteacher.

Parental Involvement

We believe that it is essential for parents / carers to be fully involved with promoting eSafety both in and outside of Academy and to be aware of their responsibilities. We will regularly consult and discuss eSafety with parents / carers and seek to promote a wide understanding of the benefits of new technologies, together with the associated risks.

- Parents / carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to the Academy.
- Parents / carers are required to make a decision as to whether they consent to images of their child being taken and used in the public domain (e.g., on Academy website).
- Parents / carers are expected to sign a Home School agreement containing the following statement:

  → **We will support the Academy approach to on-line safety and not deliberately upload or add any text, image, sound or videos that could upset or offend any member of the Academy community.**

- The Academy disseminates information to parents relating to eSafety in the form of:

  - Information and celebration evenings.
  - Practical training sessions e.g. How to adjust the Facebook privacy settings.
  - Posters.
  - Academy website.
  - Newsletter items.

Social Media

Facebook, Twitter and other forms of social media are increasingly becoming an important part of daily life.

- Staff **are not** permitted to access their personal social media accounts using Academy equipment **at any time.**
- Staff cannot set up social media accounts using their Academy email address. In order to be able to teach pupils the safe and responsible use of Facebook or other applications, the appropriate elements of the VLE should be used.
- Pupils are not permitted to access their social media accounts whilst on Academy premises or an external visit organised by the Academy.
- Staff, governors, pupils, parents and carers are regularly provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others.
- Staff, governors, pupils, parents and carers are aware that the information, comments, images and video they post online can be viewed by others, copied and stay online forever.
- Staff and governors should not name the Academy, reveal names of colleagues, pupils, or any persons associated with the Academy, discuss Academy business or disclose other confidential information acquired through your job on any social networking site or social media site.
- Staff, governors, pupils, parents and carers are aware that their online behaviour must at all times be compatible with UK law.

PERSONAL AND PROFESSIONAL CONDUCT (from Teacher Standards 1.9.12)

A teacher is expected to demonstrate consistently high standards of personal and professional conduct. The following statements define the behaviour and attitudes which set the required standard for conduct throughout a teacher's career.

- Teachers uphold public trust in the profession and maintain high standards of ethics and behaviour, within and outside school, by:
    - treating pupils with dignity, building relationships rooted in mutual respect, and at all times observing proper boundaries appropriate to a teacher's professional position
    - having regard for the need to safeguard pupils' well-being, in accordance with statutory provisions
    - showing tolerance of and respect for the rights of others
    - not undermining fundamental British values; including democracy, the rule of law, individual liberty and mutual respect, and tolerance of those with different faiths and beliefs
    - ensuring that personal beliefs are not expressed in ways which exploit pupils' vulnerability or might lead them to break the law.
- Teachers must have proper and professional regard for the ethos, policies and practices of the school in which they teach, and maintain high standards in their own attendance and punctuality.
- Teachers must have an understanding of, and always act within, the statutory frameworks which set out their professional duties and responsibilities.

Data Security

The management and appropriate use of Academy data is something that the Academy takes very seriously.

Security

- The Academy gives relevant staff access to its Management Information Systems, with a unique username and password.
- It is the responsibility of everyone to keep passwords secure.
- Staff are aware of their responsibility when accessing Academy data.
- Staff have been issued with the relevant guidance documents and the Policy for ICT Acceptable Use.
- The SLT have identified an Information Risk Owner (IRO) and Asset Information Owner(s) (AIO).
- Staff must keep all Academy related data secure. This includes all personal, sensitive, confidential or classified data.
- Staff must avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight.
- Staff must always carry portable and mobile ICT equipment or removable media as hand luggage, and keep it under your control at all times.
- It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents faxed, copied, scanned or printed. This is particularly important when shared mopiers (multi-function print, fax, scan and copiers) are used.

Protective Marking

- Appropriate labelling of data / media should help to secure data and so reduce the risk of security incidents.
- Applying too high a protective marking can inhibit access, lead to unnecessary and expensive protective controls, and impair the efficiency of an organisation's business.
- Applying too low a protective marking may lead to damaging consequences and compromise of the asset.
- The sensitivity of an asset may change over time and it may be necessary to reclassify assets. If a document is being de-classified or the marking changed, the file should also be changed to reflect the highest marking within its contents.
- We recommend 3 levels of labelling:
    - Unclassified (*or if unmarked*) – this will imply that the document contains no sensitive or personal information and will be a public document.
    - Protect – this should be the default setting and be applied to documents containing any sensitive or personal data. Marking documents as Protect will demonstrate an awareness of the Data Protection Act and the Academy's responsibilities.
    - Restricted – documents containing any ultra sensitive data for even one person should be marked as Restricted.

Information Risk Owner (IRO)

The IRO is a senior member of staff who is familiar with information risks and the Academy's response and has the following responsibilities for information management:

- owns the information risk policy and risk assessment.
- appoints the Information Asset Owner(s) (IAOs).
- acts as an advocate for information risk management.

Our Academy IRO is Sandra Wolfe.

Information Asset Owner (IAO)

Any information that is sensitive needs to be protected. This will include the personal data of learners and staff, such as assessment records, medical information and special educational needs data. All such data should be assigned an Information Asset Owner, for example, the Academy's Management Information System (MIS) is the responsibility of the MIS Officer.

The role of an IAO is to understand:

- what information is held, and for what purposes.
- what information needs to be protected. How information will be amended or added to over time.
- who has access to the data and why.
- how information is retained and disposed of.

As a result, the IAO is able to manage and address risks to the information and make sure that information handling complies with legal requirements.

Although these roles have been explicitly identified, the handling of secured data is everyone's responsibility – whether they are an employee, consultant, software provider or managed service provider. Failing to apply appropriate controls to secure data could amount to gross misconduct or even legal action.

Protecting Personal / Confidential Information

- Ensure that any Academy information accessed from your own PC or removable media equipment is kept secure.
- Ensure you lock your screen before moving away from your computer during your normal working day to prevent unauthorised access.
- Ensure the accuracy of any personal, sensitive, confidential and classified information you disclose or share with others.
- Ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person.
- Ensure the security of any personal, sensitive, confidential and classified information contained in documents you fax, copy, scan or print. This is particularly important when shared mopiers (multi-function print, fax, scan and copiers) are used and when access is from a non-Academy environment.
- Only download personal data from systems if expressly authorised to do so by your manager.
- You must not post on the internet personal, sensitive, confidential, or classified information, or disseminate such information in any way that may compromise its' intended restricted audience.
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information.
- Ensure hard copies of data are securely stored and disposed of after use in accordance with the document labeling.

Remote Access

- You are responsible for all activity via a remote access facility.
- Only use equipment with an appropriate level of security for remote access.
- To prevent unauthorised access to Academy systems, keep all dial-up access information such as telephone numbers, logon IDs and PINs confidential and do not disclose them to anyone.
- Select PINs to ensure that they are not easily guessed, e.g. do not use your house or telephone number or choose consecutive or repeated numbers.
- Avoid writing down or otherwise recording any network access information. Any such information that is written down must be kept in a secure place and disguised so that no other person will be able to identify what it is.
- Protect Academy information and data at all times, including any printed material produced while using the remote access facility. Take particular care when access is from a non-Academy environment.

Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the Academy community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of pupils) and staff, the Academy permits the appropriate taking of images by staff and pupils **with Academy equipment.**
- **Staff are not permitted to use personal digital equipment**, such as mobile phones and cameras, to record images of pupils. This includes when on field trips
- **Pupils are not permitted to use personal digital equipment**, including mobile phones and cameras, to record images of pupils, staff and others.
- Permission to use images of all staff who work at the Academy is sought when necessary.

Publishing

On a child's entry to the Academy, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- on the Academy web site.
- in the Academy prospectus and other printed publications that the Academy may produce for promotional purposes.
- Recorded / transmitted on a video or webcam.
- on the Academy's learning platform or Virtual Learning Environment.
- in display material that may be used in the Academy's communal areas.
- in display material that may be used in external areas, ie exhibition promoting the Academy.
- general media appearances, eg local / national media / press releases sent to the press highlighting an activity (sent using traditional methods or electronically).

This consent form is considered valid for the entire period that the child attends the Academy unless there is a change in the child's circumstances where consent could be an issue, eg divorce of parents, custody issues, etc.

Parents or carers may withdraw permission, in writing, at any time. Consent has to be given by both parents in order for it to be deemed valid.

Webcams and CCTV

- The Academy uses CCTV for security and safety. The only people with access to this are the SLT, Site Supervisor and ICT Support Manager. Notification of CCTV use is displayed at the front of the

Academy

- We do not use publicly accessible webcams in the Academy.
- Webcams in the Academy are only ever used for specific learning purposes, i.e. monitoring hens' eggs and never using images of children or adults.
- Misuse of the webcam by any member of the Academy community will result in sanctions (as listed under the ' inappropriate materials' section of this document).
- Consent is sought from parents/carers and staff on joining the Academy, in the same way as for all images.

Videoconferencing

- Permission is sought from parents and carers if their children are involved in video conferences.
- Permission is sought from parents and carers if their children are involved in video conferences with end-points outside of the Academy.
- All pupils are supervised by a member of staff when video conferencing.
- All pupils are supervised by a member of staff when video conferencing with end-points beyond the Academy.
- The Academy keeps a record of video conferences, including date, time and participants.
- Approval from the Headteacher is sought prior to all video conferences within the Academy.
- The Academy conferencing equipment is not set to auto-answer and is only switched on for scheduled and approved conferences.
- No part of any video conference is recorded in any medium without the written consent of those taking part.

Additional points to consider:

- Participants in conferences offered by 3rd party organisations may not be CRB checked.
- Conference supervisors need to be familiar with how to use the video conferencing equipment, particularly how to end a call if at any point any person taking part becomes unhappy with the content of the conference.

ICT Equipment and Infrastructure

ICT Equipment

- As a user of the Academy ICT equipment, you are responsible for your activity.
- The Academy logs ICT equipment issued to staff and records serial numbers as part of the inventory.
- Do not allow your visitors to plug their ICT hardware into the Academy network points (unless special provision has been made). They should be directed to the wireless ICT facilities if available.
- Ensure that all ICT equipment that you use is kept physically secure.
- Do not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990.
- It is imperative that you save your data on a frequent basis to the Academy's network. You are responsible for the backup and restoration of any of your data that is not held on the Academy's network.
- Personal or sensitive data should not be stored on the local drives of desktop PC, laptop, USB memory stick or other portable device. If it is necessary to do so the local drive must be encrypted
- It is recommended that a time locking screensaver is applied to all machines. Any device accessing personal data must have a locking screensaver as must any user profiles.
- Privately owned ICT equipment must not be used on the Academy network.
- On termination of employment, resignation or transfer, return all ICT equipment to your Manager. You must also provide details of all your system logons and passwords so that they can be disabled.
- It is your responsibility to ensure that any information accessed from your own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person.
- All ICT equipment allocated to staff must be authorised. by a member of the Senior Leadership team or those directed by the SLT.
- Authorising mangers are responsible for:
    - maintaining control of the allocation and transfer within their Unit.
    - recovering and returning equipment when no longer needed.
- All redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA)

Servers

- Servers are kept in a locked and secure environment.
- Access rights are limited.
- The server is always password protected and locked.
- Servers have security software installed appropriate to the machine's specification.
- Back up tapes are encrypted by appropriate software.
- Data is backed up regularly.
- Back up tapes are taken off site in a secure manner.
- Remote back ups are automatically securely encrypted.

Portable Equipment

- You are responsible for the security of your Academy mobile phone or portable device. Always set the PIN code and do not leave it unattended and on display (especially in vehicles).
- Report the loss or theft of any Academy mobile equipment immediately.
- The Academy remains responsible for all call or data costs until a device is reported lost or stolen.
- You must read and understand the user instructions and safety points relating to the use of your Academy mobile device prior to using it.
- Academy SIM cards must only be used in Academy provided mobile phones.
- All Academy mobile phones are barred from calling premium rate numbers and any numbers outside of the UK as the default.
- You must not send text messages to premium rate services.
- Never use a hand-held mobile phone whilst driving a vehicle. Only genuine 999 or 111 emergency calls may be made if it would be unsafe to stop before doing so.

Removable Media

If storing or transferring personal, sensitive, confidential or classified information using removable media, always consider if an alternative solution already exists.

- Only use recommended removable media.
- Encrypt and password protect.
- Store all removable media securely.
- Removable media must be disposed of securely by the ICT support team.

Telephone Services

- You may make or receive personal telephone calls from the telephone in the Family room

    1. They are infrequent, kept as brief as possible and do not cause annoyance to others.

    2. They are not for profit, to premium rate services or overseas.

    3. They conform to this and other relevant Academy policies.

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

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

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

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

Mobile Phones

Thames Primary Academy are well aware that many primary-age children own a mobile phone and we understand the widespread growth in modern electronic communication. However, we are an institution that is primarily focused on learning, and the safety and well-being of our pupils is paramount. Consequently we discourage children from bringing mobile phones into school.

Mobile phones for children

The school policy is that children should not bring mobile phones or any form of electronic communication devices to school.

- If a parent or guardian believes that there is a need for a child to be in possession of a mobile phone while at school they should write to the Headteacher to explain why this is so and why special dispensation should be allowed. The Headteacher will make a decision in all cases.
- If a child is found in possession of a mobile phone it will be confiscated by a member of staff for the remainder of the school day. The member of staff will keep the mobile phone in a safe place until the end of the school day when it will be returned to the child. If this happens more than once the mobile will be returned to the parent or carer so that the school can explain why mobile phones are not permitted.

The school does not allow children to use mobile phones in school because:

- there are some concerns about the health risks connected to the frequent use of mobile phones.
- their use in school may distract pupils away from their work.
- mobile phones may be misused (for example, cyber bullying, viewing the Internet inappropriately and sending or receiving inappropriate images of members of the school community).
- staff time could be taken up investigating lost or even stolen mobile phones.

Mobile phones for staff

The Academy allows staff to bring in personal mobile phones for their own use.

- During lesson times and in directed work time, personal mobile phones must be switched off or left on silent. Mobile phones should be stored in handbags, cupboards or lockers at all times when the adult is working with children and not kept on your person.
- Mobile phones are not to be used when adults are working with children.
- Staff should not use personal mobile phones to make or receive calls, text messages or emails during the working school day.
- Mobile phones can only be used for private calls and text messages outside of a member of staff's working day (working day excludes lunchtime).
- The sending of inappropriate or offensive text messages between any members of the Academy community is not permitted.

Disposal of Redundant ICT Equipment

- All redundant ICT equipment will be disposed of through an authorised agency.This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
- All redundant ICT equipment that may have held personal data will have the storage media overwritten multiple times to ensure the data is irretrievably destroyed. If the storage media has failed it will be physically destroyed. We will only use authorised companies who will supply a written guarantee that this will happen.
- Disposal of any ICT equipment will conform to the appropriate regulations.
- The Academy maintains a comprehensive inventory of all its' ICT equipment including a record of disposal.
- The Academy's disposal records include:
    - Date item disposed of.
    - Authorisation for disposal, including:
        - verification of software licensing.
        - any personal data likely to be held on the storage media.
    - How it was disposed of eg waste, gift, sale.
    - Name of person & / or / organisation who received the disposed item.
- Any redundant ICT equipment being considered for sale / gift will have been subject to an electrical safety check and hold a valid PAT certificate.

Writing and Reviewing this Policy

Staff, governors and pupils have been involved in making / reviewing the ICT Acceptable Use policies.

Review Procedure

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

There will be on-going opportunities for staff to discuss with the IRO/AIOs any issue of data security that concerns them.

This policy will be reviewed annually and consideration given to the implications for future Academy development planning.

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

This policy has been read, amended and approved by the staff, pupils, Headteacher and governors during February 2013.

Appendix 1 – Acceptable Use Agreement: Pupils

Primary Pupil Acceptable Use

Agreement / eSafety Rules

- I will only use ICT in the Academy for Academy purposes.
- I will only use my class e-mail address or my own Academy e-mail address when e-mailing.
- I will only open e-mail attachments from people I know, or who my teacher has approved.
- I will not tell other people my ICT passwords.
- I will only open/delete my own files.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not deliberately look for save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone unless this is part of an Academy project approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I will support the Academy approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the Academy community.
- I know that my use of ICT can be checked and that my parent/ carer contacted if a member of Academy staff is concerned about my eSafety.

Dear Parent/ Carer

ICT including the internet, e-mail and mobile technologies has become an important part of learning in our schoolAcademy. We expect all children to be safe and responsible when using any ICT.

Please read and discuss these eSafety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact XXXXX.the class teacher.

- - ✂ -

Parent/ carer signature

We have discussed this and ……………………………………......(child name) agrees to follow the eSafety rules and to support the safe use of ICT at Thames Primary Academy.

Parent/ Carer Signature …….………………….……………………….

Class …………………………………. Date ………………………………

Appendix 2 – Acceptable Use Agreement: Staff and Governors

Acceptable Use Agreement / Code of Conduct

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

- I will only use the Academy's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Headteacher or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the Academy or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will comply with the Academy's Mobile Phone Policy.
- I will not give out my own personal details, such as mobile phone number and personal e-mail address, to pupils.
- I will only use the approved, secure e-mail system(s) for any Academy business.
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in Academy, taken off the Academy premises or accessed remotely. Personal data can only be taken out of the Academy or accessed remotely when authorised by the Headteacher or Governing Body. Personal or sensitive data taken off site must be encrypted.
- I will not install any hardware of software without permission of the ICT Support Manager.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken and stored using Academy equipment and used for professional purposes in line with Academy policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the Academy network without the permission of the parent/ carer, member of staff or Headteacher.
- I will support the Academy approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the Academy community.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to the SLT. I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in Academy and outside Academy, will not bring the Academy or my professional role into disrepute.
- I will support and promote the Academy's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.

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

Signature …… Date …….

Full Name …….. (printed)

Job title ……

Appendix 3 – Acceptable Use Agreement: Parents and Visitors

Acceptable Use Agreement / Code of Conduct

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in the Academy. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff, parents and visitors are expected to are expected to respect the Academy code of conduct and behave in an appropriate manner at all times. Any concerns or clarification should be discussed with Julie Allison, the Academy eSafety coordinator or Sandra Wolfe, the Information Risk Owner.

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

Appendix 4 – eSafety Policy in brief

- The Academy has an Acceptable Use policy which is reviewed at least annually, and agreed by all staff. ICT Acceptable Use Agreements are signed by all staff, governors, students/visitors and pupils. Parents and visitors are made aware of the policy and the consequences of non-conformity.

- Safe Handling of Data guidance documents are issued to all members of the Academy who have access to sensitive or personal data.

- Protected and Restricted material must be encrypted if the material is to be removed from the Academy.

- We use the S2S website to securely transfer CTF pupil data files to other schools.

- All servers are in lockable locations and managed by CRB-checked staff, under the control of the ICT Support Manager.

- We use tape backup for the curriculum server, with an encrypted copy kept off-site. A secondary backup is created on NAS disks which are housed in a secure area.

- The admin server is backed up at a 3rd party remote site using an encrypted service.
  Disaster recovery of our admin server would use this remote backup service.

- Disposal: Sensitive or personal material in electronic files is securely overwritten and other media shredded, incinerated or otherwise disintegrated when disposed of. We use accredited companies for the disposal of system hard drives where any protected or restricted data has been held.
  Academy paper-based sensitive information is shredded, using cross cut shredders, either on-site or under contract by a 3rd party company.

- Laptops and iPads used by staff at home (loaned by the Academy) where used for any protected data are subject to the same policies as all other in-house ICT equipment, covering use of equipment, data security, etc

- Access to the setting-up of usernames and passwords which enable users to access data systems e.g. for email, network access, SLG and Learning Platform access is controlled by the ICT Support Manager.

- Security policies are reviewed and staff updated at least annually.

- Staff know how to report any incidents where data protection may have been compromised and have guidance documentation.

Appendix 5 – Information Risk Assessment Form

Information Asset	Information Asset Owner	Protective Marking	Likelihood	Overall risk level (low, medium, high)	Action(s) to minimise risk

Appendix 6 – Example Flowcharts for eSafety Incident Management