e-Safety Policy and Guidance

Issue Number:	1.0
Issue Date:	05/2014
Review Date:	04/2017
Reference:	SPTA/CA/ICT
Approved By:	Sir Paul Edwards
Approval Date:	19 May 2014

School Partnership Trust Academies
Unit 2, Wisconsin Drive
Carolina Court, Lakeside
Doncaster DN4 5RA
Tel: 01302 379 240
E-mail: info@schoolpartnershiptrust.org.uk

School Partnership Trust Academies, Company Number 7386086,
Charity exempt under Academies Act, VAT number 115 8112 43
Registered Office: School Partnership Trust Academies, Education
House, Unit 5, Fusion Court, Aberford Road, Garforth, Leeds LS25 2GH.
Tel: 0113 336 8615. E-mail: info@schoolpartnershiptrust.org.uk

CONTENTS

Appendices

1 Introduction

SPTA's intention in publishing an e-Safety Policy is not to impose restrictions that are contrary to SPTA's established culture of openness, trust and integrity. This policy, supported by the acceptable use agreements for staff, EAB Members, visitors and learners is designed to protect the interests and safety of the whole SPTA community. All users need to be aware of the range of risks associated with the use of ICT and related technologies.

2 Roles and Responsibilities

The Principal and EAB Members are responsible for ensuring that the policy and associated practices are embedded and monitored in Academies. Executive Leadership Team members are responsible for the implementation of this policy in the Core Improvement Team.

The Principal may nominate an e-safety coordinator. If no e-safety coordinator is nominated, the Principal will be deemed to be responsible for e-safety in their Academy.

All elements of this policy apply to Directors, EAB Members, employees, contractors, consultants, and other workers at SPTA, including all personnel affiliated with third parties. It also applies to members of the public who use or connect to SPTA equipment. This policy applies to all equipment that is owned or leased by SPTA and the use of other devices to access the SPTA network.

Any employee found to have violated any aspect of this policy and guidance may be subject to disciplinary action under SPTA's Disciplinary Procedure, up to and including termination of employment. All staff will be asked to sign an acceptable Use agreement as part of their induction process – please see **Appendix 1.**

Scope

This policy and guidance applies to both fixed and mobile internet technologies provided by SPTA or an Academy (such as PCs, laptops, personal digital assistants (PDAs), tablets, webcams, whiteboards, voting systems, digital video equipment, etc.) and technologies owned by students and staff, but brought onto Academy premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc.).

These technologies are to be used for business purposes in serving the interests of our learners and staff in the course of normal operations.

3 e-Safety in the Curriculum

- SPTA has a framework for teaching internet skills in ICT/ PHSE lessons
- SPTA provides opportunities within a range of curriculum areas to teach about e-Safety.
- Educating students on the dangers of technologies that may be encountered outside SPTA is carried out informally when opportunities arise and formally as part of the e-Safety curriculum.
- Students are made 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.
- Students are taught about copyright and respecting other people's information, images, etc. through discussion, modelling and activities.
- Students are made aware of the impact of online bullying and of how to seek help if they are affected by these issues. Students are also made aware of where to seek advice or help if they experience problems when using the internet and related technologies i.e. Learning Mentors parent/ carer, teacher/ trusted staff member, or an organisation such as Childline/ Child Exploitation and Online Protection (CEOP) report abuse button.
- Students are taught to evaluate materials critically and to learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum

Students with additional needs

SPTA endeavours to ensure that each Academy creates a consistent message with parents of all students. However, staff are aware that some students may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-Safety issues.

Where a pupil has additional needs in respect of social understanding, careful consideration should be given to group interactions when raising awareness of e-Safety. Internet activities must be planned and well managed for these children and young people.

Parental Involvement

- Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to the Academy. **Please see Appendix 2.**
- Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g. on an Academy website). **Please see section 10.**
- The Academy disseminates information to parents relating to e-Safety where appropriate in the form of:
    - Information and celebration evenings;
    - Posters;
    - Website/ Learning Platform postings;
    - Newsletter items; and
    - Learning platform training.

4 Password Security

All users are responsible for implementing password security in all aspects of creating, protecting and managing passwords. Passwords for SPTA systems must be created and managed in accordance with this policy. See **Appendix 3** for guidance

4.1 Password Disclosure

Users **must not** disclose their passwords to anyone.
Users **must not** write their passwords down under any circumstances.

Unauthorised password disclosure is deemed a serious security matter and may be dealt with under the SPTA's Disciplinary Procedure, up to and including termination of employment.

4.2 Shared Passwords

There may be rare occasions when it is necessary to share a common password between more than one user, if having individual usernames and passwords is operationally unacceptable, such as where the sharing of equipment is required, and the logout and login times required to swap users are unacceptable.

Any such arrangement **must** be authorised by the Departmental Head or Line Manager.

All access to line of business applications, including email, will be gained through the use of individual logins which will have to be entered by each user independently.

5 Data Security

The accessing of Academy data is something that SPTA takes very seriously.
Any data shared with an external body must be subject to a data sharing agreement approved by the SPTA Director of ICT.

Staff must be made aware of their responsibilities when accessing Academy data.

They **must not**:

- access data outside of Academy, except when entering assessment data;
- take copies of the data;
- allow others to view the data;
- Edit the data unless specifically requested to do so by the Principal and/ or the Education Advisory Body;
- Leave SIMS open for students to view;
- Leave their workstations unlocked when leaving the classroom;
- Allow a student to use the classroom PC; and
- Share staff passwords or store passwords insecurely.

6 Acceptable Usage

Effective security is a team effort involving the participation and support of every SPTA employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

6.1 General Use and Ownership

While the SPTA Core Information Technology Services team (CITS) wishes to provide a reasonable level of privacy, users should be aware that the data or emails they create on the corporate systems remain the property of the SPTA. Because of the need to protect the SPTA network, management cannot guarantee the confidentiality of information stored on any network device belonging to SPTA.

Employees are responsible for exercising good judgment regarding the reasonableness of personal use. If there is any uncertainty, employees should consult their supervisor or manager.

Any information that users consider sensitive or vulnerable must be encrypted. For guidelines on encrypting your information contact CITS.

For security and network maintenance purposes, authorised individuals within SPTA may monitor equipment, systems and network traffic at any time.
SPTA reserves the right to audit networks and systems on a periodic basis.

6.2 Unacceptable Use

The activities listed in **Appendix 4** are prohibited.

7 Managing the Internet Safely

SPTA monitors Internet use from all computers and devices connected to the corporate network. For all traffic, the monitoring system must record the source IP Address, the date, the time, the protocol, and the destination site or server. Where possible, the system should record the User ID of the person or account initiating the traffic. Internet Use records must be preserved for one hundred and eighty 180 days.

Core Information Technology Services (CITS) members may access all reports and data if necessary to respond to a security incident. Internet Use reports that identify specific users, sites, teams, or devices will only be made available to associates outside the CITS upon written or email request to CITS from a Human Resources Representative. Further guidance on managing the internet safely is provided in **Appendix 5**

8 Managing Email

The School Partnership Trust email system must not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair colour, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any SPTA employee should report the matter to their Line Manager immediately. Any breach of this eSafety policy may be dealt with under the SPTA's Disciplinary Procedure, up to and including termination of employment.

8.1 Personal Use.

Using a reasonable amount of School Partnership Trust resources for personal emails is acceptable, but non-work related email must be saved in a separate folder from work related email. Sending chain letters or joke emails from an SPTA email account is prohibited. Virus or other malware warnings and mass mailings from SPTA accounts must be approved by CITS before sending

8.2 Monitoring

School Partnership Trust employees shall have no expectation of privacy in anything they store, send or receive on the company's email system. SPTA may monitor messages without prior notice. SPTA is not obliged to monitor email messages.

8.3 Email Forwarding Policy

SPTA employees are provided with an SPTA email account. Employees are not permitted to use personal email accounts for SPTA business. Unless approved by an employee's Line Manager, SPTA email will not be automatically forwarded to an external email address.

9 Social networking / Web 2 Technologies

SPTA does not discourage staff and students from using such services in their own time. However, all should be aware that SPTA will take seriously any occasions where the services are used inappropriately. If online bullying or harassment is found to have taken place, these will be dealt with in accordance with the SPTA Harassment and Bullying policy.

It is important to recognise that there are also issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage staff and students to think carefully about the way that information can be added and removed by all users, including themselves, from these sites. Additional guidance for both staff and students is included in **Appendix 6**

Any serious misuse of Social Networking sites will be dealt with in accordance with the SPTA Disciplinary policy.
Guidance is provided below in respect of Facebook and Twitter. The same principles should be applied to other social networking sites such as WhatsApp and Snapchat. This list is not exhaustive.

9.1 Facebook

SPTA Academies are not permitted to have Facebook accounts.

Staff may use Facebook in their own time using their own IT assets. However:

- Under no circumstances should pupils or ex-pupils under the age of 18 be accepted as a friend. Failure to follow this will result in disciplinary action being taken. If a child requests a member of staff as a friend then the child's parents must be informed.
- Staff are asked to use extreme caution if a parent makes contact through Facebook. In the event of communicating with a parent or adult associated with a child who attends the school, an employee must not make any comments about students, staff or parents.
- Any statements or status remarks must not contain any comments about SPTA, the Academy, staff, parents or students.
- Teaching Staff should not use SPTA equipment to access social networking sites as part of their work unless prior permission has been granted by their Line Manager.

.

9.2 Twitter

SPTA Academies may use Twitter social networking as method of communication with stakeholders. This communication is permitted by SPTA providing it adheres to the following guidelines.

- The Principal is responsible for the content of the Academy Twitter feed.
- The Twitter feed must be used for Academy business only. The content must be appropriate and considered.
- Access to an Academy Twitter account will be managed by the Principal with an authorised user list available to SPTA on request.
- An administration account for all Academy Twitter feeds must be submitted to SPTA CITS upon request.
- Inappropriate content posted via Twitter will result of suspension of the account and control of the account will be taken by SPTA CITS.

10 Safe Use of Images

Digital images are easy to capture, reproduce and publish and also to misuse. 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 images for appropriateness.

With the written consent of parents (on behalf of students) and staff, Academies may permit the appropriate taking of images by staff and students with Academy equipment.

Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of students; this includes when on field trips. However with the express permission of the Principal, images can be taken provided they are transferred immediately and solely to the Academy's network and deleted from the staff device.

Students are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others; this includes when on field trips. However with the express permission of the Principal, images can be taken provided they are transferred immediately and solely to the Academy's network and deleted from the students device.

10.1 Consent of adults who work at the Academy

Permission to use images of all staff who work at the Academy should be sought on induction and a copy retained in the individual's personnel file

10.2 Publishing pupil's images and work

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

- on the Academy web site;
- on the Academy's Learning Platform/VLE;
- in the Academy prospectus and other printed publications that the Academy may produce for promotional purposes;
- recorded/ transmitted on a video or webcam;
- in display material that may be used in the Academy's communal areas;
- in display material that may be used in external areas e.g. an exhibition promoting the Academy; and
- general media appearances, e.g. 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 the child attends the Academy unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc.

Parents/ carers may withdraw permission, in writing, at any time. Consent has to be given by the person with parental responsibility to be valid.

Students' full names will not be published alongside their image. Email and postal addresses of students will not be published. Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed. No photos should be uploaded to website or put in any publications without prior checking with the Principal or nominated responsible person at the Academy.

Only SPTA or the nominated responsible person at the Academy has authority to upload images to the site. **If links to Youtube are provided a disclaimer must state that this link is to an external website and that SPTA is not responsible for the content of external sites.**

10.3 Storage of Images

Images/ films of children are stored on the Academy's network.

Students and staff are not permitted to use personal portable media for storage of images (e.g. USB sticks) without the express permission of the Principal.

Rights of access to this material are restricted to the teaching staff and students within the confines of the Academy network/ Learning Platform.

10.4 Webcams and CCTV

Please see the **SPTA CCTV policy**.

10.5 Video Conferencing

Video conferencing can provide valuable leaning opportunities but the associated risks need to be carefully considered and managed. **Appendix 7** provides specific guidance in respect of the use of video conferencing by Academies.

11 Remote Access

Mobile computing and storage devices containing or accessing the information resources at SPTA must be approved by CITS prior to connecting to SPTA information systems. This applies to all devices connecting to the network at SPTA, regardless of ownership.

Mobile computing and storage devices include, but are not limited to: laptop computers, personal digital assistants (PDAs), plug-ins, Universal Serial Bus (USB) port devices, Compact Discs (CDs), Digital Versatile Discs (DVDs), flash drives, modems, handheld wireless devices, wireless networking cards, and any other existing or future mobile computing or storage device, either personally owned or SPTA owned, that may connect to or access the information systems at SPTA.

A risk analysis for each new media type must be conducted and documented prior to its use or connection to the network at SPTA.

12 Mobile technologies, including Removable Media Devices

Removable media devices, including laptops, mobile phones, tablets and USB memory sticks are particularly vulnerable to loss and theft due to their size and portability. Users must take all reasonable precautions to prevent a security breach. Approval for access to, and use of, mobile computing and removable media devices must be given by your Line Manager or CITS. Should access to, and use of, mobile computing and removable media devices be approved, the following sections apply and must be adhered to at all times.

Special care **must** be taken to physically protect the removable media device and stored information from loss, theft or damage. Anyone using removable media devices to transfer information must consider the most appropriate way to transport the device and be able to demonstrate that they took reasonable care to avoid damage or loss.

Only information that is authorised and necessary to be transferred should be saved on to the removable media device. Users should note that information that has been deleted can still be retrieved.

Removable media devices **must not** be used for archiving or storing records as an alternative to other storage equipment.

Non-SPTA owned removable media devices **must not** be used to store any information used to conduct official SPTA business, and **must not** be used with any SPTA owned or leased IT equipment unless authorised by SPTA Core IT Services.

Further detailed guidance is provided in **Appendix 8**.

It should be noted that if a user loses or has a mobile device/tablet stolen which contains unencrypted personal data owned by SPTA, they may be liable to prosecution under the Data Protection Act 1998.

13 Misuse or Infringements

13.1 Inappropriate material

All users must be made aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the e-safety co-ordinator. The e-safety coordinator must record the incident on the e-safety log. **Please see Appendix 9.** This incident log must be monitored termly by the Principal. designated SLT member or EAB Chair.

Deliberate access to inappropriate materials by any user will lead to the incident being logged by the e-Safety co-ordinator. Depending on the seriousness of the offence further action taken may include:

- investigation by the Principal/ Education Advisory Body;
- immediate sanctions, possibly leading to exclusion/dismissal; or
- involvement of police for very serious offences.

Users are made aware of sanctions relating to the misuse or misconduct through inductions (staff) and ICT lessons (students).

14 Anti-Virus

All SPTA PCs must have the SPTA's standard, supported anti-virus software installed and scheduled to run at regular intervals. In addition, the anti-virus software and the virus pattern files must be kept up-to-date. Virus-infected computers must be removed from the network until they are verified as virus-free. Academy Technical Leads are responsible for creating procedures that ensure anti-virus software is run at regular intervals, and computers are verified as virus-free. Any activities with the intention to create and/or distribute malicious programs into SPTA's networks (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are prohibited.

15 Computer Use

Appropriate measures must be taken when using computers to ensure the confidentiality, integrity and availability of sensitive information and that access to sensitive information is restricted to authorised users.

Employees using computers must consider the sensitivity of the information that may be accessed and minimise the possibility of unauthorised access.

Appropriate measures include:

- Restricting physical access to computers to only authorised personnel;
- Securing computers (screen lock or logout) prior to leaving an area to prevent unauthorised access;
- Enabling a password-protected screen saver with a short timeout period to ensure that computers that were left unsecured will be protected;
- Ensuring computers are used for authorised business purposes only;
- Never installing unauthorised software on computers; and
- Ensuring that monitors are positioned away from public view. If necessary, privacy screen filters or other physical barriers to public viewing will be installed.

16 Clear Screen

All users are expected to log off from their PCs/ laptops when left for long periods and overnight.

When leaving their desk for lunch or to attend a meeting, users should lock down their screen using Ctrl, Alt, Del and then selecting Lock Workstation. SPTA systems will do this automatically after 15 minutes; however taking this measure will further reduce any security risk. **NOTE: Academies may need longer than 15 minutes to cover timeout during lessons. This should be discussed and agreed with CITS before implementation.**

Mobile devices through which access to the network can be obtained, for example Ipads, should be PIN protected, set to power off after a period of within 5 minutes and switched off when left unattended. These devices should be stored securely when not in use.

17 Complaints

Complaints relating to e-Safety should be made to the e-Safety co-ordinator or Principal. E safety incidents should be recorded using the log in **Appendix 9.**

18 Review

This policy will be reviewed every three years, or when there are changes to relevant legislation.

Acceptable Use Agreement: SPTA Staff, EAB Members and Visitors

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in SPTA and its Academies. All staff are expected to sign this agreement and adhere at all times to its contents. Any concerns or clarification should be discussed with the Academy e-Safety coordinator.

- 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 Principal or Education Advisory 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 students and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address, to students.
- I will only use the approved, secure email system(s) for any Academy business.
- I will ensure that personal data (such as data held on SIMS) 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 Principal or the Education Advisory Body.
- I will not install any hardware of software without permission of the ICT technician.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of students and/ or staff will only be taken, stored and used for professional purposes in line with Academy policy and with the 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 Principal.
- 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 Principal.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in Academy and outside Academy, will not bring my professional role into disrepute.
- I will support and promote the Academy's e-Safety policy and help students 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 use of ICT throughout the Academy.

Signature …….…… Date ……

Full Name …….....(printed)

Job title . . . . . .

Appendix 2 Acceptable use agreement - Learners

Acceptable Use Agreement / e-Safety Rules

- I will only use ICT systems in Academy, including the internet, email, digital video, mobile technologies, etc. for Academy purposes.
- I will not download or install software on Academy technologies.
- I will only log on to the Academy network/ Learning Platform with my own user name and password.
- I will follow the Academy's ICT security system, will not reveal my passwords to anyone and will change them regularly.
- I will only use my Academy email address while at the Academy or while using the Academy's equipment.
- I will make sure that all ICT communications with students, teachers or others is responsible and sensible.
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher.
- I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone unless this is part of an Academy project approved by my teacher.
- Images of students and/ or staff will only be taken, stored and used for Academy purposes in line with Academy policy and not be distributed outside the Academy network without the permission of the Principal.
- I will ensure that my online activity, both in Academy and outside Academy, will not cause my Academy, the staff, students or others distress or bring it into disrepute.
- I will respect the privacy and ownership of others' work on-line at all times.
- I will not attempt to bypass the internet filtering system.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to my teachers.
- I understand that these rules are designed to keep me safe and that if they are not followed, Academy sanctions will be applied and my parent/ carer or the Police may be contacted.

Student Signature

I agree to follow this Code of Conduct and to support the safe use of ICT throughout the Academy.

Signature …….…… Date ……

Full Name ……..(printed)

Year . . . . . .

Appendix 3 Password characteristics and guidelines

Password characteristics and guidelines

Passwords **must** be composed of the following characteristics:

- The password is at least **eight (8)** alphanumeric characters long for non-critical and non-admin accounts.
- Critical Systems/user password should not be less than **fifteen (15)** alphanumeric characters (e.g. Built-in Admins, domain admins, and service accounts) whenever possible.
- The password must contain both upper and lower case characters (e.g., a-z, A-Z)

The password must contain at least one numeric digit (e.g. 0-9). Passwords **should NOT** have the following characteristics:

- A word found in a dictionary or a word in any language, slang, dialect, jargons etc.
- Passwords shall not be the same as the username, login id, or Payroll number.
- Default or generic passwords should not be used.
- Passwords with common usage words such as: Password, Letmein etc.
- Common names, family, pets, friends, co-workers, celebrities, famous historical figures…etc.
- Computer terms and names, commands, sites, companies, hardware, software.
- Personal information, addresses, birthdays, email, phone number etc.
- Patterns such as abcdef, ASDFGH, zyxwvuts, 123321, 123456, 98765 etc.
- Any of the above spelled backwards.
- Any of the above preceded or followed by a digit (e.g. secret1,1secret)

Creating memorable passwords:

- One way to do this is by creating a password based on a song title, poems, affirmation, or other common phrase. (e.g., the phrase might be: "This May Be One Way to Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

Password Expiry

All staff passwords will be forced to expire after **seventy two (72) d**ays when possible.

Password expiry notifications will be generated prior to expiry with ample time (at least **3 days** or at most **6 logins**) and reminders to change when possible.

Passwords cannot be changed by the user until they are more than **one (1)** day old. Repetitive password change by the user within the same day should be disabled when possible to prevent password history breaches.

Appendix 3 Password characteristics and guidelines

User Account Lockout

User accounts will be locked out for **fifteen (15)** minutes if **five (5**) incorrect passwords are entered.

For certain secured applications passwords may be changed when user access accounts are locked out more than **one (1)** time per **thirty-six (36)** hour period.

Password Reset

A user requiring a password reset for access to the standard SPTA desktop must contact the CITS (Core IT Services) and provide sufficient detail to assure the service desk that their request is genuine.

A user requiring a password reset for access to a secured system must contact the CITS Service Desk, which may request further authorisation from the user department or system administration team dependant on the security policy for that particular application.

When the user uses the password provided by the ICT Service Desk they **MUST** change the password immediately at the next login.

Password History

Users may not re-use passwords they have previously used when their password expires. The password history will be the minimum of **twenty (20)** passwords when possible.

If the CITS Service Desk needs user/desktop access so that they can gain physical access for work such as application installation or reimaging they will reset the password to a temporary one. Once the Service Desk team have completed their investigations they will inform the user of the temporary password which will have been set to expire at next login. The user should use the temporary password and change it immediately at the next login.

Application Developers

Application developers must **NOT** disclose their application development standards.

Application developers must ensure their programs contain the following security precautions.

- Support authentication of individual users, not groups.
- Do not store passwords in clear text or in any easily reversible form.
- Provide for role based management to prevent privilege escalations.

Authentication Mechanisms

Information systems will authenticate all users. Passwords will be used as a base level of authentication.

Functions with high privilege and risk require strong multi-factor authentication, involving a password as well as one or more different authentication factors. Authentication options include hardware tokens, smartcards, alternative channels e.g. Public Key Infrastructure, (PKI), Certificates, Short Message Service (SMS), or call-back, one-time passwords and biometrics.

Password Entry (Network Security)

Information systems **must not** retain account or password information from previous logins.

Passwords **must not** be shown as plain-text when they are entered by a user. A common masking symbol (e.g. asterisk) shall be displayed for every typed character.

All production system-level passwords **must** be part of the administered global password management system.

User accounts that have system-level privileges granted through group memberships or programs such as "sudo" **must** have a unique password from all other accounts held by that user.

Single Sign On (SSO)

Single Sign On (SSO) provides the mechanism of accessing multiple systems with one access. However, secure systems, or systems with higher IL level data should always require a separate authentication, and **must not** be accessed via SSO.

Appendix 2 Unacceptable use

Under no circumstances is an employee of SPTA authorised to engage in any activity that is illegal under UK or international law while utilising SPTA-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by SPTA.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which SPTA or the end user does not have an active license.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
- Introduction of malicious programs into the network or server (e.g. viruses, worms, Trojan horses, e-mail bombs, etc.).
- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- Using an SPTA computing asset to engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.
- Making fraudulent offers of products, items, or services originating from any SPTA account.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Port scanning or security scanning is expressly prohibited unless prior notification to SPTA is made.

- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
- Circumventing user authentication or security of any host, network or account.
- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
- Providing information about, or lists of, SPTA's employees to outside parties.

Email and Communications Activities

The following activities are strictly prohibited, with no exceptions:

- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
- Unauthorized use, or forging, of email header information.
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Use of unsolicited email originating from within SPTA's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by SPTA or connected via the SPTA network.
- Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services). Any exemption **must** be approved by your Line Manager **before** it is used.

Internet Use Filtering System

CITS will block access to Internet websites and protocols that are deemed inappropriate for SPTA's environment. The following protocols and categories of websites will be blocked:

- Adult/Sexually Explicit Material;
- Advertisements & Pop-Ups;
- Chat and Instant Messaging;
- Gambling;
- Hacking;
- Illegal Drugs;
- Intimate Apparel and Swimwear;
- Peer to Peer File Sharing;
- Personals and Dating;
- Social Network Services;
- SPAM, Phishing and Fraud;
- Spyware;
- Tasteless and Offensive Content;
- Violence, Intolerance and Hate; and
- Certain, non-approved, Web Based Email.

Internet Use Filtering Rule Changes

The CITS will periodically review and recommend changes to web and protocol filtering rules. Changes to web and protocol filtering rules will be recorded in CITS protocols and will be available on request to employees of SPTA.

Internet Use Filtering Exceptions

If a site is mis-categorised, employees may request the site be un-blocked by submitting a change request to CITS. CITS will review the request and un-block the site if it is mis-categorised.

Employees may access blocked sites with permission if access is appropriate and necessary for business purposes. If an employee needs access to a site that is blocked and appropriately categorized, they must submit a request to their Human Resources representative or Line Manager. All requests for approval of a site must be made in writing or by email to CITS.

Appendix 6 Social networking guidance

Students

- All students are advised to be cautious about the information given by others on sites, for example users not being who they say they are.
- Students should avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- Students are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, academy details, IM/ email address, specific hobbies/ interests).
- Students are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Students are encouraged to be wary about publishing specific and detailed private thoughts online.
- Our students are asked to report any incidents of bullying to a member of staff at the Academy.

Employees

- Staff may only create blogs, wikis or other web 2 spaces in order to communicate with students using the VLE or other systems approved by the Principal.
- An individual is free to talk about SPTA and or their Academy. However instances of SPTA or the Academy being brought into disrepute may constitute misconduct or gross misconduct and disciplinary action will be taken.
- An employee must not disclose confidential information relating to his/her employment at the SPTA.
- Sites must not be used to verbally abuse staff or students. Privacy and feelings of others should be respected at all times. Employees should obtain the permission of individuals before posting contact details or pictures. Care should be taken to avoid using language which could be deemed as offensive to others.
- If information on the site raises a cause for concern with regard to any conflict of interest, employees should raise the issue with their Line Manager.
- If approached by a media contact about content on a site relating to the SPTA, employees should advise their line manager before taking any action.
- Viewing and updating personal sites must not take place during working time unless agreed in advance as appropriate by your Line Manager. Access to Facebook is not permitted through any internet connection managed by the SPTA CITS (Core Information Technology Services) unless authorisation is obtained from CITS or your Line Manager.
- Sites must not be used for accessing or sharing illegal content. Blogging from SPTA's systems is subject to monitoring

Appendix 7 Video conferencing guidance

Video Conferencing – guidance

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 students are supervised by a member of staff when video conferencing.

All students 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 Principal is sought prior to all video conferences within 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 DBS 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.

Appendix 8 Mobile technologies guidance

Mobile technologies – guidance

Laptops

In order to minimise the potential risks, users must apply the following security controls:

- The physical security of laptops is the personal responsibility of users who must take all reasonable precautions and be sensible and stay alert to the risks.
- Users **must** keep laptops within their possession within sight whenever possible. They should never be left unattended in public view. Extra care should be taken in public places such as airports, railway stations or restaurants.
- Where possible, laptops should be locked out of sight and must never be left unattended in a vehicle in public view. If absolutely necessary, it should be locked out of sight in the boot but it is generally safer for the user to take it with them.
- Laptops should be carried and stored in a padded laptop computer bag or strong briefcase to reduce the chance of accidental damage. An ordinary-looking briefcase is also less likely to attract thieves than an obvious laptop bag.
- In the event of loss or theft the Police must be notified immediately and SPTA Core IT Service Desk informed as soon as practicable.
- Information should not be stored on local hard drives unless there is no alternative. Protectively marked information must not be stored on the hard drive unless it is encrypted.
- Data encryption may be applied to all laptop hard drives owned by SPTA.

Tablets, mobile phones and USB Sticks

These remain the property of SPTA. In order to minimise any potential risks, users must apply the following security controls:

- Personal devices **must not** be connected to a laptop or desktop for any other purpose than re-charging the device.
- No protectively marked information may be stored on a Mobile device unless it is encrypted and the device is locked with a PIN code.
- It is the user's responsibility to ensure that sensitive information, including that contained in emails, is not be held on a mobile device for longer than is necessary.
- All spam, chain and other junk emails are subject to the SPTA's email policy.
- The downloading of unauthorised software on to a SPTA Device is prohibited.
- Employees **must** report any suspected virus to the SPTA Core ICT Service desk immediately.

Employees must take all appropriate steps to protect the mobile device from loss, theft or damage. These steps include, but are not limited to:-

- The mobile device **must not** be left unattended in public view in a vehicle,

Appendix 8 Mobile technologies guidance

- The mobile device **must not** be left unattended in a public place.
- The keypad **must** be locked at all times when the mobile device is not in use.
- All mobile devices **must** be password/pin protected.
- Users should be aware that SPTA may deploy software to monitor the use of removable media devices and the transfer of information to and from all removable media devices and SPTA-owned IT equipment. It may prohibit the use of devices that have not been recorded on the SPTA IT Asset Register. Management reports may be generated and used to support internal and external audit.
- Damaged, faulty or infected devices must not be used.
- Up-to date virus and malware checking software must be operational on both the machine from which the information is taken and the machine on to which the data is to be loaded. In order to implement this, it is necessary to regularly plug laptops into the SPTA network.
- If whilst using removable media the checking software indicates there is a problem, use of the device must be stopped immediately and SPTA Core ICT Services informed so it can be recorded as an incident.

Appendix 9 E safety incident log

Details of all e Safety incidents to be recorded by the eSafety Coordinator. This incident log will be monitored termly by the Principal, member of SLT or Chair of EAB.

Date and Time	Name of pupil or staff member	Male or female	Room and computer / device number	Details of incident (including evidence)	Actions and reasons