e-safety and Data Security

Policy Ratified on	17.3.21.
Signed Chair of Governors	Angela M. Wyghton.
Signed Head Teacher	

eSafety and Data Security Policy

ICT in the 21st Century 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 need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology 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
- Learning Platforms and Virtual Learning Environments
- E-mail and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Sidestrand Hall School 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.

Schools hold 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 school. This can make it more difficult for your school to use technology to benefit learners.

Everybody in the school 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 should be made aware of the risks and threats and how to minimise them.

Both this policy and the Acceptable Use Agreements (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, personal digital assistants (PDAs), tablets, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc).

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 school, 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; 'netiquette'.

Sidestrand Hall School operates its own google for education domain which provides all school staff and pupils with an email account. These sidestrandhall.net accounts are monitored at school level and any suspected misuse or inappropriate words generate an alert to the school's designated E-Safety monitors, The Head Teacher, Designated Safeguarding Lead, and the ICT Services Manager.

Managing e-Mail

- Staff are provided with their own e-mail account to use for all school business as a work based tool. This is to 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 school email account should be the account that is used for all school business
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses
- All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes
- E-mails created or received as part of your School job 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 in school.
    - Keep up to date your contacts of school staff
- 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, virus checking attachments
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail and Staff must inform the school ICT Service Manager if they receive an offensive e-mail

- Pupils are introduced to e-mail as part of the ICT Scheme of Work
- However you access your school e-mail (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply
- The use of Hotmail, BTInternet, AOL, personal Gmail, or any other Internet based webmail service for sending, reading or receiving business related e-mail is not permitted

Sending e-Mails

- 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 the shared drive rather than sending attachments
- School 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 school ICT Service Manager.
- Do not use the e-mail systems to store attachments. Detach and save business related work to the appropriate shared drive/folder
- The automatic forwarding and deletion of e-mails is not allowed

E-mailing Personal, Sensitive, Confidential or Classified Information

- Assess whether the information can be transmitted by other secure means before using e-mail - e-mailing confidential data is not recommended and should be avoided where possible
- The use of Hotmail, BT Internet, AOL or any other Internet based webmail service for sending e-mail containing sensitive information is not permitted
- Where your conclusion is that e-mail must be used to transmit such data:
    - Obtain express consent from a member of the school senior leadership team to provide the information by e-mail
    - Exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:
    - 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 send the information to anybody/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

E-mail Additional Security

When sending an e-mail containing personal or sensitive data you need to put a security classification in the first line of the e-mail. For e-mails to do with information about a pupil, for example, you need to put in PROTECT – PERSONAL on the first line of the e-mail.

This also needs to go on the top of any documents that you send i.e. Word documents, reports, forms, including paper documents you send in hardcopy etc. The name of the individual is not to be included in the subject line and the document containing the information encrypted. This provides additional security.

Internet Access

The Internet is an open communication medium, available to all, 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.

Staff and pupils connect to the Internet using the schools secured network. Filtering and security systems are in place from county (see section Infrastructure). Additional filtering and security is also in place on site, including;

a. Netsweeper, a web filtering system which the School ICT department can block or unblock additional websites and;
b. AB Tutor, a monitoring program which can monitor any computer on site and snapshot keystrokes of inappropriate words. Any questionable activity will be immediately referred to a member of the Senior Leadership Team and/or Child Protection Officer by the ICT Services Manager.

The school operates a Guest Wi-Fi system for outside professionals visiting our site. This system is not filtered through Netsweeper and therefore is not recommended for use by staff and pupils. Guests requesting to use this system will only be given log in details once they have agreed to the Schools Acceptable Use for Guest Wi-Fi Agreement (appendix 5)

Managing the Internet

- The school allows pupils supervised access to Internet resources through the school's fixed and mobile internet technology
- 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 school software or illegal software from other sources
- All users must observe copyright of materials from electronic resources
- Temporary unblocking of certain sites, such as Facebook may take place while teaching Online and E-safety.
- Where Internet use is a Safeguarding concern, the ICT Department will unblock sites to validate an issue with permission from a Designated Safeguarding Lead.
- Concerns/comments/incidents regarding social media and electronic devices must be reported to SLT and parents must be involved in any follow up action where these are out of school hours and premises. Pupils have an entitlement to privacy.

Internet Use

- You must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise its intended restricted audience
- Don't reveal names of colleagues, customers or clients or any other confidential information acquired through your job on any social networking site or blog
- Online gambling or gaming is not allowed

It is at the Head Teacher's discretion on what Internet activities are permissible for staff and pupils and how this is disseminated.

Infrastructure

School internet access is controlled through the Local Authority web filtering service. Any questionable activity will be immediately referred to a member of the Senior Leadership Team and/or Child Protection Officer by the ICT Services Manager. Sidestrand Hall School is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998

- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required
- The school does not allow pupils access to internet logs
- The school 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 teacher. The incident will then be reported by the teacher immediately to the ICT Service Manager
- As part of the school's annual support contract with ICT Solutions, antivirus software is installed and updated on all school windows based machines.
- Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility to install or maintain virus protection on personal systems. If pupils wish to bring in work on removable media it must be given to the (ICT Service Manager/teacher) for a safety check first
- Pupils and staff are not permitted to download programs or files on school equipment without seeking prior permission from (the Headteacher/member of the Senior Leadership Team/ ICT Service Manager)
- If there are any issues related to viruses or anti-virus software, the ICT Service Manager should be informed

Managing Other Web 2 Technologies

Web 2, 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 school endeavours to deny access to social networking sites to pupils within school

- All pupils are advised to be cautious about the information given by others on sites, 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 sites 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 such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, email address, specific hobbies/ interests)
- Our pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts online
- Our pupils are asked to report any incidents of bullying to the school
- Staff are not permitted to create blogs, wikis or other web 2 spaces in order to communicate with pupils. Any communication to pupils via blogging should be done via the school website, which has the facility in place for staff to post blogs which are then screened by the Head Teacher or ICT Services Manager prior to publication.

Staff Professional Responsibilities

Staff when using any form of ICT, including the Internet, in school and outside school. For your own protection the school advise that you shall:

- Ensure all electronic communication with pupils, parents, carers, staff and others is compatible with your professional role and in line with school policies.
- Do not talk about your professional role in any capacity when using social media such as personal blogs, Facebook, Twitter or YouTube.
- Do not put online any text, image, sound or video that could upset or offend any member of the whole school community or be incompatible with your professional role.
- Use school ICT systems and resources for all school business. This includes your school email address, camera/video equipment and telephone/mobile.
- Do not give out your own personal details, such as mobile phone number, personal e-mail address or social network details to pupils, parents, carers and others.
- Do not give out or publish your personal contact details, including links and address to personal blogs or social media accounts, within signatures of email sent from your school email account.
- Do not disclose any passwords and ensure that personal data is kept secure and used appropriately.
- Only take images of pupils and/ or staff for professional purposes, in accordance with school policy and with the knowledge of the school Senior Leader Team. Equipment will be provided by school and personal cameras, mobile phones, etc should not be used (see Use of Photographs and Video Policy).
- Do not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Ensure that your online activity, **both in school and outside school**, will not bring the school or professional role into disrepute.
- You have a duty to report any eSafety incident which may impact on you, your professionalism or your organisation.
- Any identified non-compliance/risk shall be reported to the Local Authority Designated Officer (LADO).

Monitoring

- The school Designated Safeguarding Lead and ICT Service Manager liaise regularly to discuss school issues/policy/procedures and current national/local issues/guidance.
- School ICT Service Manager may inspect any ICT equipment owned or leased by the School at any time without prior notice.
- School ICT Service Manager (instructed by Headteacher/Senior Leadership Team) 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 school pupils, employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain school business related information; to confirm or investigate compliance with school policies, standards and procedures; to ensure the effective operation of school 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.
- School ICT staff (instructed by Headteacher/Senior Leadership Team) 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 School ICT Service Manager (instructed by Headteacher/Senior Leadership Team) 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 School ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

Breaches

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

Any policy breach is grounds for disciplinary action in accordance with the School Disciplinary Procedure. Policy breaches may also lead to criminal or civil proceedings.

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 school's ICT Service Manager, Headteacher or Senior Designated Professional with Lead Responsibility for Safeguarding. Additionally, lost data, virus notifications, unsolicited emails and all other policy non-compliance must be reported to the school ICT Service Manager.

Computer Viruses

- All files downloaded from the Internet, received via e-mail or on removable media (e.g. CD, removable storage device) must be checked for any viruses using school provided anti-virus software before using them
- Never interfere with any anti-virus software installed on school ICT equipment that you use
- If your machine is not routinely connected to the school network, you must make provision for regular virus updates through the school ICT Service Manager

- If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact the ICT Service Manager immediately. The ICT Service Manager will advise you what actions to take and be responsible for advising others
that need to know

Equal Opportunities – Special Educational Needs

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

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

As some pupils have limited social understanding, careful consideration is given to group interactions when raising awareness of eSafety. Internet activities are planned and well managed for these pupils.

eSafety - Roles and Responsibilities

As eSafety is an important aspect of strategic leadership within the school, the Headteacher and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The Senior Designated Professional with Lead Responsibility for Safeguarding as a member of the senior leadership team has been designated the role as named eSafety co-ordinator All members of the school community have been made aware of who holds this post. It is the role of the eSafety co-ordinator to keep abreast of current issues and guidance through organisations such as Norfolk LA, CEOP (Child Exploitation and Online Protection) and Childnet.

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

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the following school policies: safeguarding (including child protection) , health and safety, behaviour policy, anti-bullying 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 school has a framework for teaching internet skills in ICT/ PSHE lessons
- The school provides opportunities within a range of curriculum areas to teach about eSafety
- Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the ICT/ PSHE curriculum
- Pupils 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
- Pupils are taught about copyright and respecting other people's information and images through discussion, modelling and 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 an organisation such as Childline

eSafety Skills Development for Staff

- Our staff receive regular information on eSafety issues via staff team meetings
- New staff receive information on the school's acceptable use policy as part of their induction
- All staff have been made aware of 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 school community (see enclosed flowchart)
- All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas

Managing the School 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 school year
- eSafety and Childline posters are prominently displayed within the school environment.

Parental Involvement

We believe that it is essential for parents/carers to be fully involved with promoting eSafety both in and outside of school and also to be aware of their responsibilities. We regularly consult and discuss eSafety with parents/carers and seek to promote a wide understanding of the benefits related to ICT and associated risks.

- Parents/ carers and pupils are actively encouraged to contribute to adjustments or reviews of the school eSafety policy via the school council and parent/carer consultation
- Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school
- 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 school website)
- Parents/ carers are expected to sign a Home School agreement containing the following statement,
    - We will support the school approach to on-line safety and not deliberately upload or add any images, sounds or text that could upset or offend any member of the school community
- The school disseminates information to parents relating to eSafety where appropriate in the form of,
    - Information and celebration evenings
    - Posters
    - Website/postings
    - Newsletter items

Passwords and Password Security

Passwords

- Always use your own personal passwords to access computer based services
- 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 staff when necessary, and never to anyone else. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished
- Passwords must be difficult to guess
- User ID and passwords for staff and pupils who have left the School are removed from the system

Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The pupils are expected to keep their passwords secret and not to share with others, particularly their friends. Staff and pupils are regularly reminded of the need for password security.

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-safety Policy and Data Security
- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks. Including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked.
- Due consideration should be given when logging into the school network

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

Safe Use of Images

For full guidelines, see the **Use of Photographs and Video Policy**

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 school community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school 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. However, with the express permission of the Head teacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device
- Pupils 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 Head teacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the pupil's device

Consent of Adults Who Work at the School

Permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file

Publishing Pupil's Images and Work

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

- on the school web site
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, ie exhibition promoting the school
- 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 period each school year; unless there is a change in the child's circumstances where consent could be an issue, eg divorce of parents, custody issues, etc.

Parents/ 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.

Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published.

Staff who have received appropriate training have access to contribute updates to the schools website, a check needs to be made to ensure that permission has been given for work to be displayed. Once submitted, this will be reviewed by the ICT Service Manager and published. Only the school ICT Service Manager has authority to publish to the site.

Storage of Images

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

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

Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network

Staff have the responsibility of deleting the images when they are no longer required, and should delete unnecessary photos by the end of each school year. Images can be removed at the discretion of the ICT Service Manager if required.

School ICT Equipment including Portable & Mobile ICT Equipment & Removable Media

School ICT Equipment issued to staff procedures

- As a user of ICT, you are responsible for any activity undertaken on the school's ICT equipment provided to you
- The school logs ICT equipment issued to staff and record serial numbers as part of the school's inventory
- Do not allow your visitors to plug their ICT hardware into the school network points (unless special provision has been made). They should be directed to the wireless ICT Facilities
- 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 school's network drive. You are responsible for the backup and restoration of any of your data that is not held on the school's network drive
- Personal or sensitive data should not be stored on the local drives of desktop PCs. If it is necessary to do so the local drive must be encrypted
- Privately owned ICT equipment should not be used on a school 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 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 the appropriate Line Manager. Authorising Managers are responsible for:
    - maintaining control of the allocation and transfer within their area of responsibility
    - 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)

Portable & Mobile ICT Equipment

This section covers such items as laptops, PDAs and removable data storage devices. Please refer to the relevant sections of this document when considering storing or transferring personal or sensitive data

- All activities carried out on school systems and hardware will be monitored in accordance with the general policy
- Staff must ensure that all school data is stored on school's network, and not kept solely on the laptop. Any equipment where personal data is likely to be stored must be encrypted

- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey
- Synchronise all locally stored data, with the central school network server on a frequent basis
- Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades
- The installation of any applications or software packages must be authorised by the ICT Service Manager and be fully licensed
- In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight
- Portable equipment must be transported in its protective case if supplied

Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and Smart phones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile Devices (including mobile/smart phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device
- Pupils are allowed to bring personal mobile devices/phones to school but must be handed into the form tutor at registration
- The school is not responsible for the loss, damage or theft of any personal mobile device
- The sending of inappropriate text messages between any member of the school community is not allowed
- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device

School Provided Mobile Devices (including phones)

- The sending of inappropriate text messages between any member of the school community is not allowed
- Permission must be sought before any image or sound recordings are made on the devices of any member of the school community
- Where the school provides mobile technologies such as phones, laptops and PDAs for offsite visits and trips, only these devices should be used
- Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school

Removable Media

- If storing/transferring personal, sensitive, confidential or classified information using Removable Media
- Only use recommended removable media
- Store all removable media securely
- Removable media must be disposed of securely by your ICT support team

Smile and Stay Safe Poster

eSafety guidelines to be displayed throughout the school (Appendix 4)

Current Legislation

Acts Relating to Monitoring of Staff email

Data Protection Act 1998

The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.

http://www.hmso.gov.uk/acts/acts1998/19980029.htm

The Telecommunications (Lawful Business Practice)

(Interception of Communications) Regulations 2000

http://www.hmso.gov.uk/si/si2000/20002699.htm

Regulation of Investigatory Powers Act 2000

Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

http://www.hmso.gov.uk/acts/acts2000/20000023.htm

Human Rights Act 1998

http://www.hmso.gov.uk/acts/acts1998/19980042.htm

Other Acts Relating to eSafety

Racial and Religious Hatred Act 2006

It a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of "Children & Families: Safer from Sexual Crime" document as part of their child protection packs.

For more information www.teachernet.gov.uk

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

The Computer Misuse Act 1990 (sections 1 – 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to gain:

- access to computer files or software without permission (for example using another persons password to access files)
- unauthorised access, as above, in order to commit a further criminal act (such as fraud)
- impair the operation of a computer or program
- UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without

obtaining them author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 – 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Acts Relating to the Protection of Personal Data

Data Protection Act 1998

http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1

The Freedom of Information Act 200

http://www.ico.gov.uk/for_organisations/freedom_of_information_guide.aspx

Appendices

Appendix 1 Pupil Acceptable Use Agreement / eSafety Rules

Appendix 2 Letter to parent/carer Pupil Acceptable Use Agreement / eSafety Rules

Appendix 3 Staff, Governor and Visitor Acceptable Use Agreement / Code of Conduct

Appendix 4 SMILE and Stay Safe Poster

Appendix 5 Guest Wi-Fi Acceptable Use Agreement

Appendix 1

Sidestrand Hall School

Pupil Acceptable Use Agreement / eSafety Rules

- I will only use ICT in school for school purposes.
- I will only use my own school 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 a school 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 school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community
- I know that my use of ICT can be checked and that my parent/carer contacted if a member of school staff is concerned about my eSafety.

Appendix 2

USE ON SSH LETTER HEADING

Dear Parent/ Carer

ICT including the Internet, learning platforms, e-mail and mobile technologies have become an important part of learning in our school. We expect all pupils to be safe and responsible when using any ICT. It is essential that pupils are aware of e-Safety and know how to stay safe when using any ICT.

Pupils are expected to read and discuss this agreement with their parent or carer and then to sign and follow the terms of the agreement. Any concerns or explanation can be discussed with their Teacher or ICT Service Manager.

Please return the bottom section of this form to school for filing.

✂ -

Pupil Acceptable Use Agreement/eSafety Rules

We have discussed this and .... (child name)

.... (Class) agrees to follow the eSafety rules and to support the safe use of ICT at Sidestrand Hall School.

Pupil Signature ....

We will support the school approach to e safety and not deliberately upload or add any images, sounds or text on-line that could upset or offend any member of the , school community

Parent/Carer Signature .... Date ....

Appendix 3

Sidestrand Hall School

Staff, Governor and Visitor 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 school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Head Teacher or ICT Service Manager.

- 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 school 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 school business.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head teacher or Senior Leadership Team. Personal or sensitive data taken off site must be encrypted. Advice on securing data can be obtained from the school ICT Service Manager.
- I will not install any hardware of software without permission of a member of the ICT Service 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, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Head teacher.
- I will not use personal equipment (such as cameras, mobile phones, tablets) for recording of photographs, videos, audio. Equipment will be provided by school (see Use of Photographs and Video Policy).
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community
- I understand that all my of use school computers, the Internet and other related technologies can be monitored and logged and can be made available, on request, to my

Head teacher or the Senior Designated Professional with Lead Responsibility for Safeguarding.

- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety and Data Security policy and help pupils to be safe and responsible in their use of ICT and related technologies.

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school

Signature: ..... Date .....

Full Name: .... (printed)

Job title: .....

Appendix 4

Staying safe means keeping your personal details private, such as full name, phone number, home address, photos or school. Never reply to ASL (age, sex, location)

Meeting up with someone you have met online can be dangerous. Only meet up if you have first told your parent or carer and they can be with you.

Information online can be untrue, biased or just inaccurate. Someone online my not be telling the truth about who they are - they may not be a 'friend'

Let a parent, carer, teacher or trusted adult know if you ever feel worried, uncomfortable or frightened about something online or someone you have met or who has contacted you online.

Emails, downloads, IM messages, photos and anything from someone you do not know or trust may contain a virus or unpleasant message. So do not open or reply.

Appendix 5

Sidestrand Hall School

Guest Wi-Fi Acceptable Use Agreement

Accessing this wireless network as a guest user is subject to the following terms:

- The School assumes no responsibility for guest user equipment or data when connecting to this wireless network;
- It is the sole responsibility of the wireless device owner/user to provide antivirus protection and to configure their device settings to provide the appropriate security to control access from other wireless users and the Internet.
- The School will not take responsibility for damages incurred for incorrect, insufficient or incomplete security settings; or lack of adequate or up-to-date virus protection;

- Guest wireless is a restricted service which is intended to provide access to public web sites only. Other web based services and programs may not work due to filtering policies in place;

- The School may routinely monitor information systems to assure the continued integrity and security of the IT network. You should also note that the School uses filtering software to endeavour to make sure that, wherever possible, unsuitable web sites are blocked, and keeps a record of all internet sites accessed.

- Guest users shall indemnify the School against all claims, damages and other losses attributable to the guest user's access to the network;

- Inappropriate use will be reported to the relevant authorities as required;

- Devices which are connected to the Guest Wi-Fi system should not be used by pupils or staff of the school without permission of the Head Teacher, Head of Care or ICT Manager;

- Keep the password you have been issued secure and do not share it with anyone else;

- No devices should be plugged into the mains when at school unless the device has been PAT tested within the last 12 months.

The following list is not exhaustive, but is to provide a framework for activities which fall into the category of unacceptable use. The following activities are strictly prohibited:

- Accessing inappropriate or offensive Internet sites is strictly forbidden (this will include the accessing of gambling or betting sites). Users must also report any instances of access to pornography or other offensive sites on the Internet if they become aware of it;

- Unauthorised copying of copyrighted material including digitisation and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation or distribution of any copyrighted software;

- Deliberate introduction of malicious programs into the network, fileservers or workstations (e.g. viruses, scanners, 'hacking' tools, password crackers, etc.); and

- Effecting security breaches or disruptions of network communication. This includes accessing data of which you are not an intended recipient, logging into a server or account that you are not expressly authorised to access, using network scanning

software to probe other devices connected to the network or carrying out activities that consume excessive amounts of bandwidth.

Usage of the guest wireless network is entirely at the risk of the user. By connecting to this network you agree to comply with the terms detailed above.

Signature: ..... Date .....

Full Name: .....

Company/Organisation: .....