Silverstone CE Primary School

Acceptable Use Policy Incorporating On-Line Safety

Introduction

This policy sets out our school's principles and strategies on e-safety. It was developed following staff consultation and is based on best practice recommended by the Children and Young People's Service - CYPS, Northamptonshire Police, the Northamptonshire Safeguarding Children's Board Northamptonshire, Governors, Parents/Carers and Children following CEOP Guidelines.

Policy Statement

IT and the internet have become integral to teaching and learning within our schools; providing children, young people and staff with opportunities to improve understanding, access online resources and communicate with the world all at the touch of a button. At present, the internet based technologies used extensively by young people in both home and school environments include:

- Websites
- Social Media
- Mobile phones
- Tablets
- Online gaming
- Learning Platforms and Virtual Learning Environments
- Email, Instant Messaging and Chat Rooms

Whilst this technology has many benefits for our school community, we recognise that clear procedures for appropriate use and education for staff and pupils about online behaviours, age restrictions and potential risks is crucial.

At Silverstone CE Primary School we have a duty to ensure that pupils are protected from potential harm both within and beyond the school environment. Every effort will be made to safeguard against all risks, however it is likely that we will never be able to completely eliminate them. Any incidents that do arise will be dealt with quickly and according to policy to ensure that pupils and staff continue to be protected. In accordance with Ofsted requirements young people need to be empowered and educated to make healthy and responsible decisions when using the internet in particular social media.

PLEASE NOTE: Whilst our school acknowledges that we will endeavour to safeguard against all risks we may never be able to completely eliminate them. Any incidents that may arise will be dealt with quickly and according to policy to ensure our children continue to be protected and this policy would be reviewed as appropriate.

Aims

- To ensure the safeguarding of all children and young people at Silverstone CE Primary School by detailing appropriate and acceptable use of all on-line technologies.
- To outline the role and responsibility of everyone in our school community.

- To ensure adults are clear about procedures for misuse of any technologies both within and beyond the school or educational setting.
- To develop links with parents/carers and the wider community ensuring input into policies and procedures with continued awareness of the benefits and potential issues related to technologies.

Roles and Responsibilities of the School

All staff need to feel confident in the use of new technologies and have a shared responsibility to ensure that our pupils are able to use the internet and related technologies appropriately and safely as part of the wider duty of care to which all who work in schools are bound. Staff will receive annual training in online-safety and be given opportunities to discuss issues and develop appropriate teaching methods.

Governors and Headteacher

It is the overall responsibility of the Headteacher with the Governors to ensure that there is an overview of online-safety (as part of the wider remit of Child Protection) across the school with further responsibilities as follows:

- The Headteacher has designated the On-line Safety Leader to implement agreed policies, procedures, staff training, curriculum requirements and take the lead responsibility for ensuring e-Safety is addressed in order to establish a safe digital learning environment.
- Time and resources will be provided for the On-line Safety Leader and staff to be trained and update policies during the course of each school year.
- The Headteacher is responsible for promoting on-line safety across the curriculum and has an awareness of how this is being developed, linked with the whole school development plan.
- The Headteacher will inform the governors at the Premises Committee meetings about the progress of or any updates to the on-line safety curriculum (via PSHE or computing) and ensure Governors know how this relates to child protection. At the Academic Governance Committee Meetings, all Governors will be made aware of on-line safety developments from these meetings.
- The AUP will be reviewed annually by the governors and Headteacher to ensure it defines the user rules, roles, procedures and responsibilities for on-line safety in our school.
- Ensure that any misuse or incident has been dealt with appropriately, according to policy and procedures (see the Allegation Procedure – Section 12 of Northamptonshire Safeguarding Children's Board) and appropriate action is taken, even to the extreme of suspending a member of staff, informing the police (following procedures) or involving parents/carers.

On-line Safety Leader

The designated On-Line Safety Leader will:

- Ensure that the AUP is reviewed annually
- Keep all members of our school community up-to-date with information and resources on on-line safety(as they become available)

- Work with the technican to ensure that filtering is set to the correct level for staff and children, in the initial set up of our network, stand-a-lone PCs, staff/children laptops and the learning platform (VLE)
- Remind all adults that they need to be aware of the importance of filtering content and how these filters keep us all protected.
- Report any issues that arise and update the Headteacher on a regular basis.
- Liaise with the PSHCE Co-ordinator and Designated Safeguarding Leads so that policies and procedures are up-to-date to take account of any emerging issues and technologies.
- Update staff training according to new and emerging technologies so that the correct on-line safety information can be taught or adhered to.
- Ensure all staff are aware they should not be using their own personal equipment in school for work purposes.
- Keep an up to date record of staff acceptable user forms and a record of any school equipment used at home for school business
- Keep a log of incidents for analysis to help inform future development and safeguarding, where risks can be identified. Refer to Section 12 of

the Allegation Procedure from the NSCB to ensure the correct procedures are used with incidents of misuse.

- Work alongside the ICT technician and staff to ensure there is appropriate and up-to-date anti-virus software on the network, stand-a-lone PCs and teacher/child laptops and that this is reviewed and updated on a regular basis.

Staff

It is the responsibility of all adults within the school setting to:

- Ensure that they know who the Designated Safeguarding Leads within school are so that any misuse or incidents can be reported which involve a child. Where an allegation is made against a member of staff it should be reported immediately to the Headteacher. In the event of an allegation made against the Headteacher, the Chair of Governors must be informed immediately. (Following the Allegation Procedure, Section 12, NSCB.)
- Be familiar with the Behaviour and other relevant policies so that in the event of misuse or an allegation, the correct procedures can be followed, immediately. In the event that a procedure is unknown, they will refer to the Head teacher immediately, who should then follow the Allegations Procedure, Section 12, LSCBN.
- Alert the On-Line Safety Leader of any new or arising issues that may need to be included within policies and procedures.
- Ensure that children are protected and supported in their use of on-line technologies so that children know how to use them in a safe and responsible manner.
- Be up-to-date with on-line safety knowledge that is appropriate for the age group and reinforce through the curriculum.
- Sign either a hard copy or an electronic copy of an Acceptable User form to show that they agree with and accept the rules for staff using school equipment, within and beyond the school environment, as outlined in the appendices.
- Use electronic communications in an appropriate way that does not breach the Data Protection Act 1998.
- Remember confidentiality and not disclose information from the network, pass on security passwords or leave a station unattended when they or another user is logged in.
- Report accidental access to inappropriate materials to the on-line safety Leader in order that inappropriate sites are added to the restricted list.

- Use and regularly update anti-virus software and check for viruses on their teacher laptop, memory stick or a CD ROM when transferring information from the internet on a regular basis, especially when not connected to the school network.

Children

Children are:

- Involved in the review of our acceptable use rules through the school council in line with this policy being reviewed and updated.
- Responsible for following the Acceptable Use Rules whilst within school as agreed at the beginning of each academic year or whenever a new child attends the school for the first time.
- Taught to use the internet in a safe and responsible manner through computing lessons and through cross curricular links
- Taught to tell an adult about any inappropriate materials or contact from someone they do not know straight away, without reprimand.
- Are aware of what to do if something they access on the internet is offensive or upsetting. *(see appendices for copy of our rules)*

IT Technician

The IT technician is responsible for ensuring:

- That the IT infrastructure at both schools is secure and not open to misuse or malicious attack.
- That anti-virus software is installed and maintained on all school machines and portable devices.
- That the school's filtering policy is applied and updated on a regular basis and that responsibility for its implementation is shared with the On-Line Safety Lead and the Designated Person for Safeguarding.
- That any problems or faults relating to filtering are reported to Designated Person for Safeguarding and to the broadband provider immediately and recorded on the On-Line Safety Incident Log.
- That users may only access the school's network through a rigorously enforced password protection policy, in which passwords are regularly changed.
- That he/she keeps up to date with e safety technical information in order to maintain the security of the school network and safeguard children and young people.
- That the use of the school network is regularly monitored in order that any deliberate or accidental misuse can be reported to the On-Line Safety Lead.

Appropriate Use by Staff

Staff members have access to the network so that they can access age appropriate resources for their classes and create folders for saving and managing resources.

They have a password to access our network and our filtered internet service and know that this should not be disclosed to anyone or leave their computer or device unattended whilst they are logged in.

All staff will receive a copy of the Acceptable Use Policy and a copy of the Acceptable User Form, which will need to be signed, returned to school to keep under file and a signed copy returned to the member of staff.

The Acceptable Use Rules will be displayed in the staff room as a reminder that staff members need to safeguard against potential allegations and a copy of this policy is available in the green school policies folder.

In the Event of Inappropriate Use

If a member of staff is believed to have misused the internet or learning platform in an abusive or illegal manner, a report must be made to the Headteacher immediately and then the Allegations Procedure (Section 12, NSCB) and the Child Protection Policy must be followed to deal with any misconduct and all appropriate authorities contacted.

In the lesser event of misuse or accidental misuse refer to appendices for a list of actions relating to the scale of misuse.

Appropriate Use by Children

Acceptable Use Rules and the letter for children and parents/carers are outlined in the Appendices and these rules outline how children are expected to use the internet and other technologies within school, which includes downloading or printing of any materials. The rules are there for children to understand what is expected of their behaviour and the attitude needed when using the internet which then enables them to take responsibility for their own actions. For example, knowing what is polite to write in an e-mail to another child or understanding what action to take should there be the rare occurrence of sighting unsuitable material.

The rules will be on display in all teaching areas as a reminder.

We want our parents/carers to discuss our on-line safety rules with their child, and reinforce the importance of e-safety. Each year, when we do our school data collection, a covering letter and a copy of the rules are sent to each pupil. If a pupil joins us later in the school year these are included in the new starter induction pack.

We expect all pupils and their parents/carers to sign a copy of the acceptable rules together so that it is clear to the school the rules are accepted by the child with the support of the parent/carer. These rules are also intended to provide support and information to parents/carers when children may be using the internet beyond school.

Further to this, we hope that parents/carers will add to future amendments or updates to the rules so that they feel the rules are appropriate to the technologies being used at that time and reflect any potential issues that parents/carers feel should be addressed, as appropriate.

The downloading of materials, for example, music files and photographs need to be appropriate and 'fit for purpose' based on research for work and be copyright free.

File-sharing via e-mail, weblogs or any other means online should be appropriate and be copyright free when using the learning platform in or beyond school.

In the Event of Inappropriate Use

Should a child be found to misuse the internet or e-mail facilities whilst at school the procedure outlined in the appendices should be followed and if any consequences are required these will follow those outlined in our behaviour policy. In addition:

- Any child found to be misusing the internet by not following the Acceptable Rules will have a letter sent home/telephone call to parents/carers inviting them into school so we can explaining the reason for suspending their child's use for a particular lesson.
- Further misuse of the rules will result in not being allowed to access the internet for a period of time and another letter will be sent home to parents/carers.

In the event that a child accidentally accesses inappropriate materials the child will report this to an adult immediately and turn off their screen or minimise the window (dependent on age) so that an adult can take the appropriate action. Where a young person feels unable to disclose abuse or sexual requests to an adult they will be informed how to use the Report Abuse button to make a report and seek further advice.

Pupils with additional learning needs

We strive to provide access to a broad and balanced curriculum for all learners and recognise the importance of tailoring activities to suit the educational needs of each pupil. Where a pupil has specific learning requirements, or poor social understanding, careful consideration is given to the planning and delivery of on-line safety awareness sessions and internet access.

The Curriculum and Tools For Learning

Using the internet is part of the curriculum and is a fantastic and necessary tool for learning. It is part of everyday life for education, business and social interaction. The school has a duty in providing pupils with quality internet access as part of their learning experience. Staff use age appropriate search engines such as 'Safe Search For Kids' for Key Stage 1.

Silverstone CE Primary School strives to embed On-Line Safety in all areas of our curriculum and key online safeguarding messages are reinforced wherever IT is used in learning. At school pupil usage of the internet is always supervised however filtering at school and at home is only a small safeguarding intervention. Pupils use the internet widely outside of school and need to learn how to evaluate internet information for themselves and take full responsibility for their safety and experience.

Pupils are made aware that the internet is filtered and monitored and understand the consequences of accessing inappropriate material.

On-line safety is part of the Computing and PSHE curriculum and is an ongoing learning process. The schools' use resources from the online safeguarding programmes from CEOP (Think U Know) for all year groups.

Internet Use

We teach our children how to use the internet safely and responsibly, for researching information, exploring concepts, deepening knowledge and understanding and communicating effectively in order to

further learning, through Computing and/or PSHE lessons where the following concepts, skills and competencies have been taught by the time they leave Year 6:

- internet literacy
- making good judgements about websites and e-mails received
- knowledge of risks such as viruses and opening mail from a stranger
- access to resources that outline how to be safe and responsible when using any on-line technologies
- knowledge of copy write and plagiarism issues
- file-sharing and downloading illegal content
- uploading information – know what personal information it is safe to upload and not upload

Personal safety – ensuring information uploaded to web sites and e-mailed to other people does not include any personal information including:

- full name (first name is acceptable, without a photograph)
- address
- telephone number
- e-mail address
- school
- clubs attended and where
- age or DOB
- any other information which would make it easy for a stranger to identify a child or locate their whereabouts

Photographs should only be uploaded on the approval of a member of staff or parent/carer and should only contain something that would also be acceptable in 'real life'. Parents/carers should monitor the content of photographs uploaded.

E-mail Use

We have e-mail addresses for children to use, as a class and/or as individuals depending on the age group of the pupils as part of their entitlement to being able to understand different ways of communicating and using IT to share and present information in different forms.

Staff and children are to use their school issued e-mail addresses for any communication between home and school only. Parents/carers are encouraged to be involved with the monitoring of e-mails sent.

Internet Access and Age Appropriate Filtering and Safeguarding Measures

Broadband Provider: RM Education

All students are entitled to safe and secure internet access and schools have a duty to deliver this as part of the learning experience. The Head teacher is ultimately responsible for ensuring that the school infrastructure and network is as safe and secure as is reasonably possible and that age appropriate internet filtering is in place to protect young users from inappropriate or harmful online content. To this end, the school has the following filtering measures in place:

- Filtering levels are managed and monitored in school via an administration tool/control panel, provided by our broadband supplier, which allows an authorised staff member to instantly allow or block access to a site or specific pages and manage user internet access.
- Filtering levels are managed and monitored on behalf of the schools by our broadband supplier or technical support, allowing an authorised school staff member to allow or block access to site and manage user internet access.
- Age appropriate content filtering is in place across the schools, ensuring that staff and pupils receive different levels of filtered internet access in line with user requirements (e.g. Youtube at staff level but blocked to students)
- All users have unique usernames and passwords to access the schools' network which ensures that they receive the appropriate level of filtering. Class log-ins, dependent on age, may also be used.
- Any changes to filtering levels are documented on the Filter Change Request Log and include the reason for the requested change, the date and name of staff member concerned. For audit trail purposes, signed consent from the On-Line Safety Lead must be received before the request can be actioned.

In addition to the above, the following safeguards are also in place:

- Anti-virus software is used on all network and stand alone PCs or laptops and is updated on a regular basis.
- A firewall ensures that information about pupils cannot be accessed by unauthorised users.
- Encryption codes on wireless systems prevent hacking
- The CEOP Report Abuse button is available on each schools' network to allow pupils or staff to report online safeguarding issues.
- CEOP's Hector Protector (KS1) and the CEOP report abuse button (KS2) is in use on all devices accessed by students to provide a shield for pupils should they access inappropriate content at any point.

Staff

- Expectations for staff online conduct is addressed in the Acceptable Use Policy for School based employees.
- Staff are required to preview any websites before use, including those which are recommended to students and parents for homework support.

Monitoring

School technical staff monitor user activity, including any personal use of the school IT system

Use of School and Personal IT Equipment

School IT Equipment

- A log of all IT equipment issued to staff, including serial numbers, is maintained by the School Business Manager
- Personal or sensitive data will not be stored on school devices (e.g. laptops, ipads, PC or USB Memory Sticks).

Personal IT Devises

Pupil use:

- Pupils are not permitted to bring mobile devices onto school grounds unless express permission has been granted by the Head Teacher for exceptional circumstances. However children may bring in their mobile phones into school as a safety precaution for travelling home at the end of the school day. Any pupil mobile device must be switched off once on school grounds and must be handed to their class teacher, who will keep them in a secure location.
- Pupils are not permitted to take mobile devices on school trips.

Staff use:

Personal mobile devices are permitted on school grounds, but should be used outside of lesson time only.

- It is the responsibility of the staff member to ensure that there is no illegal or inappropriate content stored on their device when brought onto school grounds.
- Personal mobile devices must not be used to contact pupils or their families, nor should they be used to take videos or photographs of pupils. School issued devices **only** should be used in these situations.

Laptops/ iPads

- Staff must ensure that all sensitive school data is not stored on the laptop or device. In the event of loss or theft, failure to safeguard sensitive data could result in a serious security breach and subsequent fine. Password protection alone is not sufficient.
- Personal use of school laptops or computing facilities, whilst on site, is left to the discretion of the Head Teacher and may be permissible if kept to a minimum, used outside of lesson times and does not interfere with an employee's work.
- Staff are provided with laptops to allow for school related work to be completed off site. Personal use of the laptop from home (such as web browsing/online shopping etc) is permitted but should be kept to a minimum and use of the device is strictly restricted to the authorised member of staff only (i.e. not family members)
- Staff are aware that all activities carried out on school devices and systems, both within and outside of the school environment, will be monitored in accordance with this policy.
- Staff will ensure that school laptops and devices are made available as necessary for anti-virus updates, software installations, patches, upgrades or routine monitoring/servicing.

Photographs and Video

Digital photographs and videos are an important part of the learning experience for pupils and, as such**,** schools have a responsibility to ensure that they not only educate students about the safe and appropriate use of digital imagery, but also model good practice themselves. To this end, there are strict policies and procedures for staff and pupils about the use of digital imagery within school. The school policy for use of images on its website can be found in the appendices of this document.

- Written consent will be obtained from parents or carers before photographs or videos of pupils will be taken or used within the school environment, including the school website or associated marketing material.
- Permission will be sought from any staff member before an image or video is taken and the purpose of the activity and intended use of the image will be made clear.

- Staff are not recommended to use personal devices, such as cameras, video equipment or camera phones, to take photographs or videos of students. However, in exceptional circumstances, permission may be granted by the Head Teacher for use of personal equipment for school related photographs or videos, provided that the there is an agreed timescale for transfer and deletion of the image from the staff member's device. (24 hours)
- Where photographs of students are published or displayed (e.g. on the school website) no names are used.
- Wherever possible, group shots of pupils will be taken, as opposed to images of individuals and images should never show young people in compromising situations or inappropriate clothing (e.g. gym kit, swimming costumes)

Video conferencing

- Permission is obtained from parents and carers prior to their child's involvement in video conferencing.
- All pupils are supervised by a member of staff when video conferencing, particularly when communicating with individuals or groups outside of the school environment (e.g. international schools)
- All video conferencing activities are time logged and dated with a list of participants.

Parents' Roles

The On-Line safety policy is accessible for parents on the school web-site. On-Line safety awareness sessions are held for parents and regular updates on On-Line safety are given through school newsletters and on the school website. Parents are asked to also sign the Acceptable Use Rules used by pupils. Each child will receive a copy of the Acceptable Use Rules on an annual basis, or first-time entry to the school, which needs to be read with the parent/carer, signed and returned to school confirming both an understanding and acceptance of the rules.

It is expected that parents will explain and discuss the rules with their child so that they are clearly understood and accepted.

Links to other Policies, Behaviour and Anti-Bullying Policies

Behaviour Policy

Please refer to the Behaviour Policy for the procedures in dealing with any potential bullying incidents via any on-line communication, such as mobile phones, e-mail or blogs.

Cyberbullying

Cyberbullying is best defined as "The use of Information and Communications Technology (ICT), particularly mobile phones and the internet, deliberately to upset someone else". DCSF 2009

The majority of adults and young people find using the internet and mobile phones a positive and creative part of everyday life. Sadly technologies can also be used in a very negative way. Often when young people are the target of bullying via mobile phones, gaming, social media, apps and chat rooms, they can often feel very isolated and very alone particularly if they feel adults around them don't understand how

cyberbullying is affecting them. Young people, school staff, practitioners, parents and carers need to understand how destructive cyberbullying can be and how it differs from other forms of bullying. It is very important that promoting a culture of confident users will support online safety.

Often bullying takes place outside the school gates but is usually brought into school and reported. If this is the case it should be reported and acted on. The DFE guidance on Preventing and tackling bullying 2014 states teachers have the power to discipline pupils for misbehaving outside the school premises "to such an extent as is reasonable". This can relate to any bullying incidents occurring anywhere off the school premises, such as on school or public transport, outside the local shops, or in a town or village centre. Furthermore The Education Act 2011 gives wider search powers to tackle cyber-bullying by providing a specific power to search for and, if necessary, delete inappropriate images (or files) on electronic devices, including mobile phones.

Cyberbullying along with any other forms of bullying by any member of the school community will not be tolerated. Any incidents of cyberbullying are recorded and reported. All concerns and incidents will be recorded by staff in class pupil/parent books. If incidents occur regularly these incidents will be logged more formally via the deputy or head teachers to form a bigger picture and as evidence for parents/governors/external agencies if needed. All staff are aware of the procedures that are in place to deal with incidents of cyberbullying. (Anti-Bullying Policy).

Allegation Procedures and the Safeguarding Policy
Please refer to the Allegation Procedure, in order to deal with any incidents that occur as a result of using personal mobile or e-mail technologies which may result in an allegation of misuse or misconduct being made by any member of staff or child about a member of staff. This procedure is also detailed in the school's staff code of conduct.

Allegations should be reported to the Headteacher immediately or Chair of Governors in the event of the allegation made about the Headteacher.

The (now DfE) DCFS White Paper clearly stated that no personal equipment belonging to staff should be used when contacting children and young people about homework or any other school issues either in or beyond school and any such action should be dealt with.
We follow these guidelines to protect our staff members from potential allegations of misconduct by a child or parent/carer.

Please refer to the Child Protection Policy (Section 12 NSBC) for the correct procedure in the event of a breach of child safety and inform the designated person for child protection within school immediately.

Incident Reporting

Internet technologies and electronic communications provide children and young people with exciting opportunities to broaden their learning experience and develop creativity inside and outside of school. However e-safety risks can be experienced deliberately or unintentionally by acting inappropriately or even illegally.

All staff are the first line of defence and all e-safety concerns must be reported. In the event of misuse by staff or pupils, including use of a school brought electronic device off site in an illegal, unsuitable or abusive manner, a report must be made to the Head teacher/Designated Person for Safeguarding immediately.

Circumstances when e-safety concerns should be reported to the Police or discussed with the designated safeguarding officer are highlighted below:

- Radicalisation – For further information on prevent contact jason.farmer@northants.pnn.police.uk http://www.northamptonshirescb.org.uk/about-northamptonshire-safeguarding-children-board/news/violent-extremism-and-radicalisation/
- Online Grooming
- Hacking
- Hate Crime's
- Harassment
- Certain types of adult material
- Other criminal conduct, activity or materials

These procedures should be followed in the event of any misuse of the internet:

A. An inappropriate website is accessed inadvertently:
Report website to the On-Line Safety Leader and write in on-line safety log for the technician to contact the helpdesk filtering service for school and Local Authority so that it can be added to the banned list.

B. An inappropriate website is accessed deliberately:
Ensure that no one else can access the material by shutting down.
Log the incident in the on-line safety log.
Report to the Headteacher and On-Line Safety Leader immediately.
Headteacher to refer back to the Acceptable Use Rules and follow agreed actions for discipline in line with school staffing policy guidelines and code of conduct.
Inform the Local Authority filtering services as with A.

C. An adult receives inappropriate material:
Do not forward this material to anyone else – doing so could be an illegal activity.
Alert the Headteacher immediately.
Ensure the material is removed and log the nature of the material.
Contact relevant authorities for further advice e.g. police.

D. An adult has used ICT equipment inappropriately:
Follow the procedures for B.

E. An adult has communicated with a child or used ICT equipment inappropriately:
Ensure the child is reassured and remove them from the situation immediately, if necessary.
Report to Mr Bloomfield, Mrs Bodman-Knight or Mrs.Watkins, the Designated Safeguarding Leads for Child Protection immediately, who should then follow the Allegations Procedureand Child Protection Policy from Section 12, NSBC.

Preserve the information received by the child if possible and determine whether the information received is abusive, threatening or innocent.

Once Procedures and Policy have been followed and the incident is considered innocent, refer to the Acceptable Use Rules for Staff and Headteacher to implement appropriate sanctions.

If illegal or inappropriate misuse is known, follow the Allegations procedure and Child Protection Policy.

Contact CEOP (police) as necessary.

In the event of minor or accidental misuse, internal investigations should be initiated and disciplinary procedures followed where appropriate. Additionally, all security breaches, lost/stolen equipment or data, unauthorised use or suspected misuse of ICT should be reported immediately to the Head Teacher.

All incidents must be recorded on the On-Line Safety Incident Log to allow for monitoring, auditing and identification of specific concerns or trends.

Where there is cause for concern that illegal activity has taken place using computer equipment, these concerns will be reported immediately to the designated safe-guarding lead and e-safety leads.

In the event of suspicion, all steps in this procedure will be followed:

- There will be more than than one senior member of staff involved in the process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Ideally use the same computer for the duration of the procedure.
- The relevant staff will have appropriate internet access to conduct the procedure. All the sites and content visited will be closely monitored and recorded as this will provide further protection.
- The URL of any site containing the alleged misuse will be recorded and also the nature of the content causing concern. If possible screen shots of the machine were the incident has taken place will be made and saved and stored. The information collated will be printed out, signed and dated.
- One this has been completed and fully investigated the safeguarding team and e-safety team or lead will judge whether the concern has substance or not. If it does then appropriate action will be required and could include the following:
- PCSO/Police referral
- Referral to the MASH team (When there are child protection concerns)
- CEOP
- CSE toolkit – To look at the risk of CSE

Bibliography

- Northamptonshire Safeguarding Children's Board
  E-Safety Guidance 2015
- Northamptonshire Acceptable Use Policy For School Based Employees
- Silverstone CE Primary School PHSE policy
- Silverstone CE Primary School Anti-Bullying policy
- Silverstone CE Primary School Behaviour policy
- Silverstone CE Primary School Computing policy
- Inspecting e-safety in schools- Ofsted

The following websites offer further information and guidance:

- www.parentscentre.gov.uk (for parents/carers)
- www.ceop.co.uk (for parents)
- www.netsmartzkids.org (5 – 17 years old)

- www.kidsmartorg.uk – (primary age and below)
- www.thinkuknow.co.uk (for primary age upwards and parents)
- www.phonebrain.org.uk (for ages 10 upwards)
- www.bbc.co.uk/dongaltherabbit (for ages 7 upwards)
- www.hectorsworld.com (younger children up to age 6 or 7 years)

APPENDICES

Silverstone CE Primary School
Acceptable Use Rules (Staff)

To ensure that all adults within our school are aware of their responsibilities when using any online technologies, such as the internet or e-mail, they are asked to sign these Acceptable Use Rules. This is so that they can provide an example to children of safe and responsible use of online technologies and remain informed, protected and safeguarded from any potential allegations or inadvertent misuse themselves.

NB: These rules apply to all online use and to anything that may be downloaded or printed.

- I know that I should only use the school equipment in an appropriate manner and for professional uses.
- I understand that I need to give permission to children before they can upload images (video or photographs) to the internet or send them via e-mail.
- I know that images should not be inappropriate or reveal any personal information of children if uploading to the internet.
- I have read the Procedures for Incidents of Misuse so that I can deal with any problems that may arise, effectively.
- I will report any incidents of concern for children's safety to the Headteacher, Mr Bloomfield, Mrs.Bodman-Knight, Mrs.Watkins the other Designated Persons for Child Protection and Designated Safeguarding Leads in accordance with procedures listed in the Acceptable Use Policy.
- I know that I am putting myself at risk of misinterpretation and allegation should I contact children via personal technologies, including my personal e-mail and should only use the **school e-mail and phones** (if provided) for school business. These should only be used to contact pupil's school e-mail addresses as agreed use within the school as part of the ICT SoW or wider connected curriculum. Parents/Carers will be encouraged to share these emails with their child/ren.
- I know that I should not be using the school system for personal use unless this has been agreed by the Headteacher and/or On-Line Safety Leader.
- I know that I should complete virus checks on my laptop and memory stick or other devices so that I do not inadvertently transfer viruses, especially where I have downloaded resources. It is my responsibility to ensure I ask the technician to update this protection annually.
- I will only install hardware and software I have been given permission for and have the correct license permissions for.
- I will not upload personal files or documents within the school server
- I will ensure that I follow the Data Protection Act 1998 and have checked I know what this involves.
- I will ensure that I keep my password secure and not disclose any security information unless to appropriate personnel. If I feel someone inappropriate requests my password I will check with the On-Line Safety Leader.
- I have read a full copy of the Acceptable Use Policy and I am aware of all identified e-safety issues and procedures that I should follow.
- I will adhere to copyright and intellectual property rights.

I have read, understood and agree with these Rules as I know that by following them I have a better understanding of e-safety and my responsibilities to safeguard children when using online technologies.

Name:_____

Signed:_____ Date: _____

Silverstone CE Primary School
Procedures to follow in the event of misuse - Children

All staff must be aware of these procedures should THEY be followed in the event of any misuse of the internet:

A. An inappropriate website is accessed inadvertently:

Pupils should be aware of how to turn off a screen or minimise a window if an inappropriate image/website is displayed.
Staff should reassure the child that they are not to blame and praise them for being safe and responsible by telling an adult. Inform the On-Line Safety Leader.
Email the website address to the technician so they can contact the helpdesk filtering service for school and LA/RBC so that it can be added to the banned list.

B. An inappropriate website is accessed deliberately:
Refer the child to the Acceptable Use Rules that were agreed.
Reinforce the knowledge that it is illegal to access certain images and police can be informed.
Decide on appropriate sanction – refer to Behaviour policy for options.
Notify the parent/carer.
Inform LA/RBC as above.

C. An adult or child has communicated with a child or used ICT equipment inappropriately:
Ensure the child is reassured and remove them from the situation immediately.
Report to the Designated Safeguarding Leads, immediately.
Preserve the information received by the child if possible, by printing chat log or covering screen, and determine whether the information received is abusive, threatening or innocent.
If illegal or inappropriate misuse the Headteacher must follow the Allegation Procedure and/or Child Protection Policy from Section 12, NSCB.
Contact CEOP (police) as necessary.

D. Threatening or malicious comments are posted to the school website or learning platform about a child in school:
Preserve any evidence, by printing chat logs or covering screen.
Inform the Headteacher immediately.
Inform the RBC/LA and On-Line Safety Leader so that new risks can be identified. Contact the police or CEOP as necessary.

Silverstone CE Primary School
On-Line Safety Rules Return Slip

2019/2020
Child's Agreement:

Name:..... Year .....

- With an adult, I have read and understood the Rules for using the internet, e-mail and online tools, safely and responsibly.
- I know that the adults working with me at school will help me to stay safe and check that I am using the computers to help me with my work.

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

Parent/Carer Agreement:

- I have read and discussed the Rules with my child and confirm that he/she has understood what the Rules mean.
- I understand that the school will use appropriate filtering and ensure appropriate supervision of children when using the internet, e-mail and online tools. I understand that occasionally inappropriate materials may be accessed and accept that the school will endeavour to ensure this is infrequent and will deal with any incident that may arise, according to policy.
- I understand that whilst my child is using the internet, e-mail and any other facilities outside of school, that it is my responsibility to ensure safe and responsible use.

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

Silverstone CE Primary School

Foundation Stage and Key Stage 1
Our Internet and E-Mail Rules

1. We use the internet safely to help us learn
2. We learn how to use the internet
3. We can send and open messages with an adult
4. We can write polite and friendly e-mails or message to people that we know
5. We only tell people on-line our first name
6. We learn to keep our password secret
7. We know who to ask for help
8. If we see something we do not like on the screen we know what to do
9. If we do not follow the rules the teacher will ring our grown ups

Silverstone CE Primary School

Key Stage 2
Our Internet and E-Mail Rules

1. We use the internet to help us learn and we will learn how to use the internet safely
2. We send e-mails and messages that are polite and friendly
3. We will only e-mail or chat to people an adult has approved
4. Adults are aware when we use online tools
5. We never give out passwords or personal information without permission (like our surname, address or phone number)
6. We never post photographs without permission and never include names with photographs
7. If we need help we know who to ask
8. If we see anything on the internet or in an e-mail that makes us uncomfortable, we know what to do
9. If we receive a message sent by someone we don't know we know what to do
10. We know we should follow the rules as part of the agreement with our parent/carer and know what will happen if we do not

Silverstone Primary School
Filtering Change Log

Website / category	Date	Requested by / reason:	Authorised/Changed by:	Confirmed by:

Silverstone CE Primary School

Incident Report Form Compiled By:

Name:

Role:

Date:

Staff Informed:

Name:

Role:

Date:

Nature of Concern:
Who was involved: Pupils/Staff/Parents?
Where did it occur: Home/School?
Time of Incident: Date of Incident:
Time the incident was logged: Date the incident was logged:

Silverstone CE Primary School
On-Line Safety Incident Log

Date of incident	Name of individual(s) involved	Device number/location	Details of incident	Actions and reasons	Confirmed by

Silverstone CE Primary School

Policy for use of images on its website

Silverstone CE Primary School has a website to promote the schools and their pupils. We wish to include images of pupils on the website and this policy lays out our practice for doing so.

This policy aims to follow best practice in the use of images of pupils on the school website. It is noted from such guidelines that:

"Including images of pupils on the school website can be motivating for the pupils involved and provide a good opportunity to promote the work of the school. It is important to balance the potential risks of including images of pupils on the website against the design principles of creating colourful, attractive and relevant pages, just as the school, heads and governors would do with any publication."

In order to protect children featured on the website we will adhere to the following guidelines:

- If an image is used, we will not name the pupil
- If the pupil is named (in an article) we will not use their image
- We will only use images of pupils in suitable dress to reduce the risk of inappropriate use
- We will only show appropriate images of pupils on the school web site

In addition to the above we will:

- have written consent to the publication of images on the Internet, via the schools' website, signed by the parent or guardian
- retain the signed consent in case it is required for reference

If there is any doubt about the suitability of an image then the Head will make a decision as to whether to use the image and where necessary consult with the parent or guardian of the child.

This e-safety policy was approved by the board of Directors/AGC/Governors Sub Committee on:	*Insert Date*
The implementation of this e-safety policy will be monitored by :	*James Bloomfield (Head-Teacher)* *Rachel Haywood(E-Safety Lead)* *Tara Fowler (E-Safety Lead)*
Monitoring will take place at regular intervals:	*Annually*
The Academic Governance Committee will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include details of e-safety incidents) at regular intervals:	
The E-Safety Policy will be reviewed annually, or more regularly due the ever changing nature of technology, new threats to technology or incidents that have taken place. The review date for policies will be:	*Insert date*
Should serious e-safety incidents take place, the following external persons/agencies should be informed:	*LEA Safeguarding Officer, Police, CEOP and MASH. CSE.*

Northamptonshire county council school e-safety audit

School: Date:

Teacher:

Action	Circle yes or no
Has the school got an e-safety policy? NB: **The e-safety policy should be integrated with other relevant policies such as behaviour, safeguarding and anti-bullying.**	Y/N
Date last updated:	
Date of future review:	
The school e-safety policy was agreed by governors on:	
The policy is available for staff to access at:	
The policy is available for parents/carers to access at:	
The responsible member of the senior leadership team is:	
The governor responsible for e-Safety is:	
The Designated Child Protection Coordinator is:	
The e-safety Coordinator is:	
Were all stakeholders (e.g. pupils, staff and parents/carers) consulted with when updating the school e-Safety Policy?	Y/N
Are teaching and non-teaching staff receiving regular and up-to-date e-Safety training?	Y/N
Do one or more members of staff have a higher level of expertise and clearly defined responsibilities?	Y/N
Do all members of staff sign an Acceptable Use Policy on appointment?	Y/N
Are all staff made aware of the schools expectation around safe and online behaviour?	Y/N
Is there a clear procedure for staff, pupils and parents/carer to follow when responding to or reporting an e-Safety incident or concern?	Y/N
Have e-safety materials from CEOP and Thinkuknow been obtained?	Y/N
Is e-safety training provided for all pupils (appropriate to age and ability and across all key stages and curriculum areas)?	Y/N
Are e-safety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all pupils?	Y/N
Do parents/carers and pupils sign an acceptable use policy?	Y/N
Are staff, pupils, parents/carers and visitors aware that network and internet use is closely monitored and individual usage can be traced?	Y/N
Is personal data collected, stored and used according to the principles of the data protection act?	Y/N
Is internet access provided by an approved educational internet service provider which complies with DfE requirements (e.g. KSPN)?	Y/N
Has the school filtering been designed to reflect educational objectives and been approved by SLT?	Y/N
Are members of staff with responsibility for managing filtering, network access and monitoring systems adequately supervised by a member of SLT	Y/N
Does the school log and record all e-safety incidents, including any action taken?	Y/N
Are the governors and SLT monitoring and evaluating the school e-Safety policy and ethos on a regular basis?	Y/N
Is the school going through or gone through an E-Safety kite mark or award?	Y/N