Smarden preschool

E-Safety Policy

February 2015

Contents

Introduction

This E-Safety Policy is intended to ensure the preschool`s documentation covers current and relevant issues, in a whole school context, linking with other relevant policies, such as the Child Protection, and Behaviour.

The School E-Safety Policy applies to all members of the school community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems and mobile technologies, both in and out of school.

E-safety Policy

Smarden preschool
Date of policy: February 2015

Policy Governance

Development, Monitoring and Review of this Policy

This e-safety policy has been developed by a working group / committee made up of:

Position	Name(s)
School E-Safety Coordinator / Officer	Katie Lipscomb
Preschool manager	Katie Lipscomb
Preschool deputy manager	Abigail Cox
Committee chair	Clare Neall
Committee treasurer	Ailsa Wilson
Parents on the committee	Clare Hardwick
	Emma Leech
	Mel Gould
	Rebecca Quinn
	Jessica Brogan

Consultation with the whole school community has taken place through the following:

Forum	Date (if applicable)
Staff meetings	*
Committee meeting	*
School website	
Newsletter	

Schedule for Review

This e-safety policy was approved by the *Committee* on:	*Date: 4th November*
The implementation of this e-safety policy will be monitored by the *Preschool manager and the committee*:	*Katie Lipscomb* *Committee*
Monitoring will take place at regular intervals:	*Once a year when updating all policies, unless any changes need to happen before hand.*
The *Committee* will receive a report on the implementation of the e-safety policy generated by the manager and the committee chair person at regular intervals:	*Once a year*
The E-Safety Policy will be reviewed *annually*, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	*Date:* Nov 2016
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	*LA Safeguarding Officer* *Police Commissioner*

Scope of the Policy

This policy applies to all members of the school community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems and mobile technologies, both in and out of school.

Roles and Responsibilities

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school:

The Committee

- Committee members are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy.

Manager and Senior Leaders:

- The manager is responsible for ensuring the safety (including e-safety) of members of the school community
- The manager and another member of the Senior Leadership Team/Senior Management Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff

E-Safety Coordinator/Officer:

- leads the e-safety committee and/or cross-school initiative on e-safety
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies/documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- reports regularly to Senior Leadership Team

Network Manager / Technical staff

is responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that the school meets the e-safety technical requirements.

- that users may only access the school's networks through a properly enforced password protection policy

Teaching and Support Staff

are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the school Staff Acceptable Use Policy/Agreement (AUP)
- they report any suspected misuse or problem to the Manager for investigation/action/sanction

Designated person for child protection/Child Protection Officer

should be trained in e-safety issues and be aware of the potential for serious child Protection issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate on-line contact with adults/strangers
- potential or actual incidents of grooming
- cyber-bullying

E-Safety Committee

Members of the E-safety Committee will assist the E-Safety Coordinator/Officer with:

- the production, review and monitoring of the school e-safety policy

Community Users

Community Users will ONLY have access to the preschool website and only suitable information and images are placed on to the website.

E-Safety Education and Training

Education & Training – Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- *A planned programme of formal e-safety training will be made available to staff It is expected that some staff will identify e-safety as a training need within the performance management process.*

- *All new staff will receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies*

Communication devices and methods

The following table shows the school's policy on the use of communication devices and methods.

Where it is indicated that the method or device is allowed at certain times, these are clearly outlined in the next table.

	Staff & other adults				Students			
Communication method or device	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
	☑	⚠	⚠	☒	☑	⚠	⚠	☒
Mobile phones may be brought to school		⚠				⚠		
Use of school ipad	☑					☑		
School Mobile			⚠					☒
Taking photos on personal mobile phones or other camera devices				☒				☒
Use of personal hand held devices eg PDAs, PSPs				☒				☒
Use of personal email addresses in school, or on school network				☒				☒
Use of school email for personal emails				☒				☒
Use of chat rooms / facilities				☒				☒
Use of instant messaging				☒				☒
Use of social networking sites				☒				☒

Use of blogs				☒				☒

 This table indicates when some of the methods or devices above may be allowed:

	Circumstances when these may be allowed	
Communication method or device	**Staff & other adults**	**Students/Pupils**
Mobile phones may be brought to school	*To be left in the staff`s tray in the office in case of emergency*	
Taking photos on personal mobile phones or other camera devices		
Use of personal hand held devices eg PDAs, PSPs		
Use of personal email addresses in school, or on school network		
Use of school email for personal emails		
Use of chat rooms / facilities		
Use of instant messaging		
Use of social networking sites		
Use of blogs		
School ipad	To be used when completing Children`s planning	

School Mobile	To be used when out of the premises on walks, or outings.	

Unsuitable/inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
User Actions	☑			☒	☒
child sexual abuse images					☒
promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					☒
adult material that potentially breaches the Obscene Publications Act in the UK					☒
criminally racist material in UK					☒
Pornography					☒
promotion of any kind of discrimination based on race, gender, sexual orientation, religion and belief, age and disability					☒
promotion of racial or religious hatred					☒
threatening behaviour, including promotion of physical violence or mental harm					☒

any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				☒	
Using school systems to run a private business				☒	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SCC and / or the school				☒	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions				☒	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				☒	
Creating or propagating computer viruses or other harmful files				☒	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet				☒	
On-line gaming (educational)				☒	
On-line gaming (non educational)				☒	
On-line gambling				☒	
On-line shopping / commerce				☒	
File sharing				☒	
Use of social networking sites				☒	
Use of video broadcasting eg Youtube				☒	
Accessing the internet for personal or social use (e.g. online shopping)				☒	
Using external data storage devices (e.g. USB) that have not been encrypted (password protected and checked for viruses				☒	

Good practice guidelines

Email

Best practice

☑ **DO**

Staff and students/pupils should only use their school email account to communicate with each other

Safe practice

Check the school e-safety policy regarding use of your school email or the internet for personal use e.g. shopping

Poor practice

☒ **DO NOT**

Staff: don't use your personal email account to communicate with students/pupils and their families without a manager's knowledge or permission – and in accordance with the e-safety policy.

Images, photos and videos

Best practice

☑ **DO**

Only use school equipment for taking pictures and videos.

Ensure parental permission is in place.

Safe practice

Check the e-safety policy for any instances where using personal devices may be allowed.

Always make sure you have the Headteacher/SLT knowledge or permission

Make arrangements for pictures to be downloaded to the school network immediately after the event.

Delete images from the camera/device after downloading.

Poor practice

☒ **DO NOT**

Don’t download images from organisation equipment to your own equipment.

Don’t use your own equipment without Headteacher/SLT knowledge or permission – and in accordance with the e-safety policy.

Don’t retain, copy or distribute images for your personal use.

Internet

Best practice

☑ **DO**

Understand how to search safely online and how to report inappropriate content .

Safe practice

Staff and students/pupils should be aware that monitoring software will log online activity.

Be aware that keystroke monitoring software does just that. This means that if you are online shopping then your passwords, credit card numbers and security codes will all be visible to the monitoring technicians

Poor practice

☒ DO NOT

Remember that accessing or downloading inappropriate or illegal material may result in criminal proceedings

Breach of the e-safety and acceptable use policies may result in confiscation of equipment, closing of accounts and instigation of sanctions.

Mobile phones

Best practice

☑ DO

Staff: If you need to use a mobile phone while on school business (trips etc), the school will should provide equipment for you.

Make sure you know about inbuilt software/ facilities and switch off if appropriate.

Safe practice

Check the e-safety policy for any instances where using personal phones may be allowed.

Staff: Make sure you know how to employ safety measures like concealing your number by dialling 141 first

Poor practice

☒ DO NOT

Staff: Don't use your own phone without the Headteacher/SLT knowledge or permission.

Don't retain service student/pupil/parental contact details for your personal use.

Social networking (e.g. Facebook/ Twitter)

Best practice

☑ DO

If you have a personal account, regularly check all settings and make sure your security settings are not open access.

Ask family and friends to not post tagged images of you on their open access profiles.

Safe practice

Don't accept people you don't know as friends.

Be aware that belonging to a 'group' can allow access to your profile.

Poor practice

☒ DO NOT

Don't have an open access profile that includes inappropriate personal information and images, photos or videos.
Staff:

- Don't accept students/pupils or their parents as friends on your personal profile.
- Don't accept ex-students/pupils users as friends.
- Don't write inappropriate or indiscrete posts about colleagues, students/pupils or their parents.

Webcams

Best practice

☑ **DO**

Make sure you know about inbuilt software/ facilities and switch off when not in use.

Safe practice

Check the e-safety policy for any instances where using personal devices may be allowed.

Always make sure you have the Headteacher/SLT knowledge or permission

Make arrangements for pictures to be downloaded to the school network immediately after the event.

Delete images from the camera/device after downloading.

Poor practice

☒ **DO NOT**

Don't download images from organisation equipment to your own equipment.

Don't use your own equipment without Headteacher/SLT knowledge or permission – and in accordance with the e-safety policy.

Don't retain, copy or distribute images for your personal use.

Incident Management

Incidents (students/pupils):	Refer to class teacher	Refer to committee	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)									
Unauthorised use of non-educational sites									
Unauthorised use of mobile phone/digital camera / other handheld device									
Unauthorised use of social networking/ instant messaging/personal email									
Unauthorised downloading or uploading of files									
Allowing others to access school network by sharing username and passwords									
Attempting to access or accessing the school network, using another accounts									
Attempting to access or accessing the school network, using the account of a member of staff									
Corrupting or destroying the data of other users									
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature									
Continued infringements of the above, following previous warnings or sanctions									
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school									
Using proxy sites or other means to subvert the school's filtering system									
Accidentally accessing offensive or pornographic material and failing to									

report the incident									
Deliberately accessing or trying to access offensive or pornography									
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act									

Incidents (staff and community users):	Refer to committee	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Removal of network / internet access rights	Warning	Further sanction
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)							
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email							
Unauthorised downloading or uploading of files							
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account							
Careless use of personal data eg holding or transferring data in an insecure manner							
Deliberate actions to breach data protection or network security rules							
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software							
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature							
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with							

students / pupils							
Actions which could compromise the staff member's professional standing							
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school							
Using proxy sites or other means to subvert the school's filtering system							
Accidentally accessing offensive or pornographic material and failing to report the incident							
Deliberately accessing or trying to access offensive or pornographic material							
Breaching copyright or licensing regulations							
Continued infringements of the above, following previous warnings or sanctions							

Staff, Volunteer and Community User Acceptable Use Policy Agreement Template

School Policy

This Acceptable Use Policy (AUP) is intended to ensure:

- that staff, volunteers and community users will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

- that staff, volunteers and community users are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff, volunteers and community users will have good access to ICT to enhance their work, to enhance learning opportunities for *staff* learning and will, in return, expect staff, volunteers and community users to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students/pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.

- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, email, VLE etc) out of school.

- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.

- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.

- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.

- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.

- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- I will not use personal email addresses on the school ICT systems.

- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.

- I will ensure that my data is regularly backed up, in accordance with relevant school policies.

- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.

- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.

- I will not disable or cause any damage to school equipment, or the equipment belonging to others.

- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School/Local Authority Personal Data Policy. Where

personal data is transferred outside the secure school network, it must be encrypted.

- I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.

- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.

- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

Staff, Volunteer and Community User Acceptable Use Agreement Form

This form relates to the student/pupil Acceptable Use Policy (AUP), to which it is attached.

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and/or the Local Authority and in the event of illegal activities the involvement of the police

- **I have read and understood the School's E-safety Policy**

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Name	

Position	
Signed	
Date	