Section 10.26

E-Safety Safer Working Practice Guidance For Those Who Work in Schools

Policy Summary

This policy provides guidance on safer working practice for schools' staff when using digital equipment and the internet.

Supporting Documents

- Responsible Use Policy
- GO Safer Working Practice Guidance (2007)
- OFSTED Thematic report: the safe use of new technologies (2009)
- Report into Nursery Z, Plymouth Safeguarding Children Board

Quality Assurance

Reviewed annually.

Circulated for comments to:

SSCB E-safety sub-group,

Version	Date	Authors	Issue Reason	Revision Date
1.0	13/10/2011	HH/ LP	New Policy	01/08/2012
1.1	11/05/2017	VS	Update	11/05/2017

Introduction

Digital technology has become an important part of everyday life and offers exciting opportunities. However the increasing number of cases where workplace practice has highlighted inappropriate use of technology, grooming behaviour and an inability to challenge colleagues has demonstrated the need for clear practice guidance for workers and organisations around safer working practice. The recent report by Plymouth Safeguarding Board into Nursery Z indicates how poor practice can go unchallenged.

http://www.plymouth.gov.uk/serious_case_review_nursery_z.pdf

As someone who works with children and young people, or adults who are their parents and carers, you should not feel that you cannot use the internet and internet enabled devices and internet packages such as social networking sites to communicate with others. However, it is essential that everyone takes care with information that is made available electronically and always remembers that once a comment or posting is made, it may not be possible to take it back. All digital records should be considered to be permanent.

As someone who works with children and young people, or adults who are their parents and carers, whether in a voluntary or paid capacity, whenever you are operating in the digital world you must always have your professional role in mind and always consider how your behaviour could affect your professional reputation and employment.

The purpose of this guidance is to provide some advice and guidance about safer working practice, keeping your personal and professional lives separate, keeping yourself safe when using electronic media and adopting responsible behaviour that should protect you from putting yourself and your career at risk. If you live and work in the same community, you should discuss how this policy affects you with your senior leader.

This guidance builds on the 'Safer Working Practice Guidance for adults working with children and their Families' issued by the Government Offices in England in 2007. A copy is available on the SSCB website.

www.safeguardingchildreninstockport.org.uk

General guidelines

- Do not behave in a way that could suggest that you are trying to develop a personal relationship with a child.

Glossary of terms

CEOP	Child Exploitation and Online Protection Centre More information from their website: www.ceop.police.uk
AUP	Acceptable Use(r) Policy This defines the rules for use; it is an agreement between the service provider (employer) and the user. Acceptable Use Policies tend to be written in ‘Do Not…’ language. For children and young people their parents may also be required to sign and agree to sanctions.
RUP	Responsible Use(r) Policy This defines the rules for use as above. It tends to be written using ‘We will…’ language.
Strong Password	A strong password contains a mixture of upper and lower case letters, numbers and other characters. It is recommended to be a minimum of 8 characters in length.
Grooming Behaviour	The psychological engagement of a sexual abuser with the intended victim to engage their involvement in the activity.

☑ DO

1. Set your privacy settings for any social networking site.

2. Ensure your mobile phone (any technological equipment) is password/ PIN protected. Use a strong password.

3. Consider having personal and professional online accounts/identities if you wish to have online contact with pupils, their families and other professionals. Then use your professional account at all times.

4. Make sure that all publicly available

☒ DO NOT

1. Give your personal information to pupils or their parents/carers. This includes mobile phone numbers, social networking accounts, personal website/blog URLs, online image storage sites, passwords etc.

2. Use your personal mobile phone to communicate with pupils. This includes phone calls, texts, emails, social networking sites, etc.

For fuller statements go to **Summary of good practice guidelines (P13)**.

Facebook/Twitter (Social Networking)

Social networking is software that enables people to stay in touch online via the internet. It provides support for sharing information, images and making contact with people who may share a common interest. It is very beguiling.

Facebook and Twitter are the most well known social networking sites but others include BEBO (Blog Early, Blog Often), MySpace, Yahoo and MSN.

Don't use your personal Facebook/ Twitter profile to communicate with or share images of pupils and their parents/ carers.

Best

Consider creating a professional profile in agreement with your head teacher/ school.

Pupils may have several profiles themselves (personal and one

Safe

Make sure your security settings are not open access but set to family and friends only.

Don't accept people you don't know as friends – they could be pupils. Go for

Consequences:
May affect your relationship with pupils or your professional status

Peer

You have an open access profile that includes inappropriate personal information and images e.g. holiday snaps, hen nights.

You accept pupils as friends on your personal profile.

You accept pupils as friends once they have

Consequences:
Breach of RUP.
May make you vulnerable to harassment,

What should be in place?

- The RUP/AUP should explicitly state that pupils and their parents/carers should not be accepted as friends and include the sanctions for the breach of this policy.
- The RUP/AUP for the organisation should include guidelines for creating/monitoring a

Email

Don't use your personal email account to communicate with pupils

Best

Your school should provide an email account for you to use for

Consequences: Poor practice blurs the professional boundaries and can make staff

Safe

Check your school's policy regarding use of

Poor

You use your personal email account to communicate with pupils and their families

What should be in place?

- RUP/AUP should be explicit about use of personal email accounts to communicate with pupils

Images

Don't use your own equipment to take images of pupils.

Best

Your school should provide equipment for you.

Know

Safe

Senior leaders agree you can use your own equipment.

Conseque nces: May result in

Poor

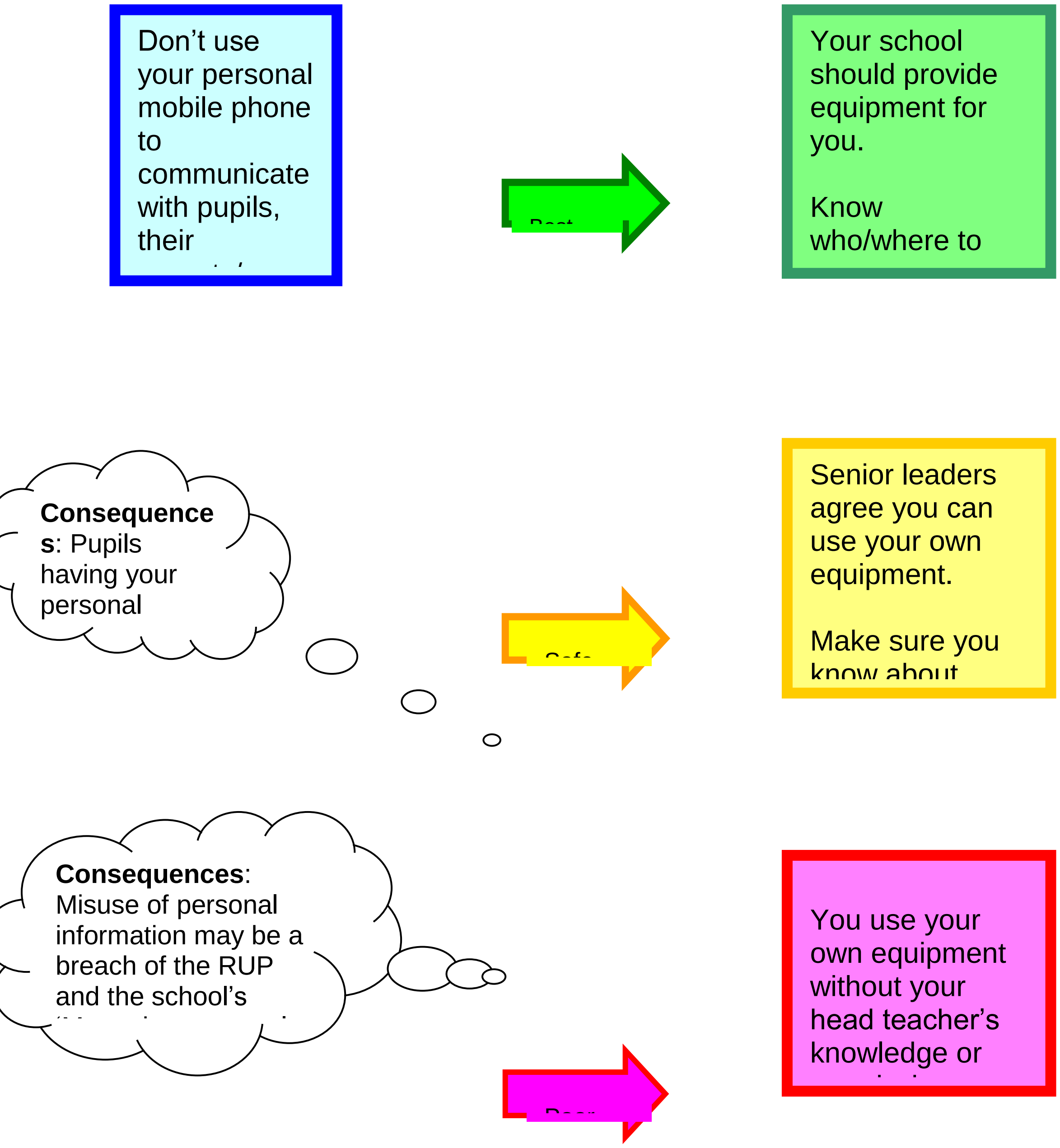
You download images from school's equipment to your own equipment.

You use your own equipment without your

What should be in place?

- Use of personal equipment should be made clear in RUP/AUP.
- Taking images of pupils should be included in RUP/AUP. Parental permission has

Mobile phones



Don't use your personal mobile phone to communicate with pupils, their

Your school should provide equipment for you.

Know who/where to

Consequences: Pupils having your personal

Senior leaders agree you can use your own equipment.

Make sure you know about

Consequences: Misuse of personal information may be a breach of the RUP and the school's

You use your own equipment without your head teacher's knowledge or

What should be in place?

- Use of personal equipment should be made clear in RUP/AUP.
- If the need for a mobile phone is for a one-off situation e.g. trip then staff know where equipment is available from and should be

Web-cams

Don't use your personal web-cam to communicate with pupils,

Best

Make sure you know about

Safe

Senior leaders agree you can use your own equipment for a specific project.

You make

Consequences: Misuse of personal information may be a breach of the AUP/RUP and the

Poor

You use your own equipment without your senior leader's knowledge or

What should be in place?

- Use of personal equipment, including webcams, should be made clear in RUP/AUP.
- If the need to use a webcam is for a one

Using the Internet

Be aware of the school's policy for the use of the internet on your work computer.

Safe

Understand how to search safely online and how to report inappropriate content either via your school's ICT section or via the CEOP report button.

Be aware that the school's monitoring

Consequences: Misuse of the internet may be a breach of the RUP. Staff may

Poor

Accessing, using or downloading

What should be in place?

- RUP/AUP make the

Summary of good practice guidelines

☑ DO

1. Set your privacy settings for any social networking site to ensure only the people you want have sight/access to the contents. Keep these updated. The default settings for most social networking sites are set to open access where anyone can see everything.

2. Ensure your mobile phone (any technological equipment) is password/PIN protected. This will ensure that other people can’t use your equipment and get you into trouble.

3. Consider having separate personal and professional online identities/accounts if you wish to have online contact with pupils, their families and other professionals. Ensure that your head teacher is aware of your professional online persona. Always use your professional account for all professional communications.

4. Make sure that all information about you that is publicly available is accurate and appropriate – think particularly about whether photographs/stories that you may have posted in your personal life are appropriate for a person with a professional life and a reputation to lose. If you don’t want it to be public, don’t put it online.

5. Remember that online conversations may be referred to as ‘chat’ but they are written documents and should always be treated as such. Be mindful about how you present yourself when you are publishing information about yourself or having ‘conversations’ on-line.

6. Make sure that you are aware of your school’s policy regarding the use of both organisational and personal digital equipment and the consequences of misuse. Understand when you need to obtain consent. Breach of the policy can result in capability/disciplinary actions by your employer, professional body and criminal proceedings by the police.

7. Err on the side of caution. If you are unsure who can view online material, assume that it is publicly available. Remember – once information is online you have relinquished control of it. Other people may choose to copy it, edit it, pass it on and save it.

8. Switch off any Bluetooth capability any device may have installed as standard. Bluetooth allows another person to have access to your equipment – they can then pretend to be you.

9. Always be aware that technology is constantly upgrading and improving. You may have access to websites via a work-provided smart phone that are blocked by your computer. Mobile phones come with locator software. Cameras can be a feature of games consoles. When you receive any new equipment (personal or private) make sure that you know what features it has as standard and take appropriate action to disable/protect.

☒ DO NOT

1. Give your personal information to pupils, their parents/carers. This includes personal mobile phone numbers, social networking accounts, personal website/blog URLs, online image storage sites, passwords/PIN numbers etc.

2. Use your personal mobile phone to communicate with pupils or parents/carers either by phone call, text, email, social networking sites.

3. Use the internet or web-based communication to send personal messages to pupils, parents/carers.

4. Share your personal details on a social network site with pupils, their parents or carers. This includes accepting them as friends. Be aware that belonging to a ‘group’ may give ‘back door’ access to your page even though you have set your privacy settings to family and friends only.

5. Add/allow pupils, their parents/carers to join your contacts/friends list on personal social networking profiles.

6. Take photographs/videos without obtaining pupil’s and/or their parent or carer’s consent.

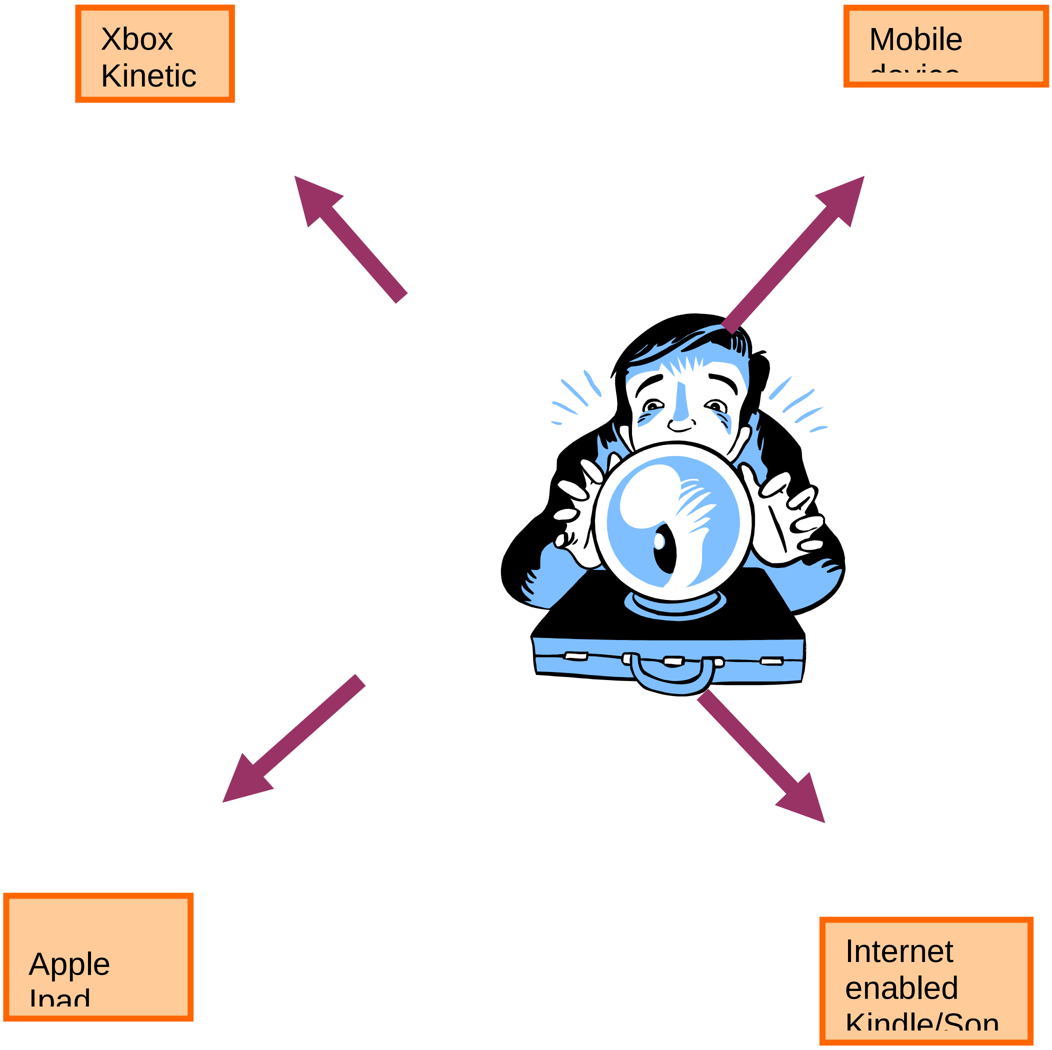
7. Use your own digital camera/video for work purposes. This includes integral cameras on mobile phones.

8. Tick the ‘remember me’ box when using password protected internet sites.

9. Play online games with pupils, their parents or carers. This can be difficult when the culture is to play with ‘*randoms*’. Check out before you play online with someone you don’t know.

Looking to the future

Technology doesn't stay still and there are devices in development and some newly launched on to the market. They will all need addressing at some point through RUP/AUP and practice guidance.



Xbox Kinetic

Mobile device

Apple Ipad

Internet enabled Kindle/Son

St Thomas' Cyber Safety Council

At St Thomas', we have an Internet Safety Council (Cyber Safety Heroes) made up of children from KS2 and the Computer Lead. The Council meet to discuss how to aid the children of the school keeping themselves safe. Here is their mission statement:

St Thomas' Cyber Safety Heroes is a group of children who aim to work alongside the children and adults of the school by:

- helping children, parents and teachers to understand how to keep safe on-line
- helping everyone to understand what cyber-safety means
- promoting respectful and good behaviour on-line
- helping everyone to become more confident with knowing how to report cyber-bullying or inappropriate behaviour
- promoting that children should spend their time doing other things other than being on computers, tablets or other devices

St Thomas' Cyber Safety Heroes Spring (Term 2017)

Terms to be aware of as they may need some action

Cyberbullying: using technology to bully people. This includes mobile phones, email, social networking and online gaming. It is especially invasive as the victim can be bullied 24/7, at anytime and in any place so there is consequently no respite. Cyberbullying can be used as a mechanism for other forms of bullying e.g. racist, sexist, and homophobic etc. Cyberbullies may bully adults as well as children.

Facebook rape/Frape/Hacking: when someone takes over your online account. Usually happens as a result of poor practice – users leave their computers logged on but move away and a passer-by seizes the opportunity to make use of the account.

Randoms: term used by players of multi-media online games (MMOG) to describe people they don't know but are opponents/allies in the online world.

Sexting: the sending of explicit sexual texts/engaging in online sexual activity e.g. over webcam. CEOP have identified a 60% increase in these 'self-generated sexual images' in 2009-10.

Tagging: where you are named in a photograph. Most associated with Facebook/Twitter. You can ask the person who has tagged you to remove the tag. Tagging might be an issue if friends/relatives post pictures of you/pupils (e.g. children cared for by the Local Authority) without your knowledge or permission.

Resources

Information Commissioner's Office
http://www.ico.gov.uk/Global/Search.aspx?collection=ico&keywords=social+networking

Parenting Online
http://www.wiredkids.org/parents/parentingonline/parentingonline.pdf

A Guide to Video Games, Parental Controls and Online Safety
http://www.esrb.org/about/news/downloads/ESRB_PTA_Brochure-web_version.pdf

Safer Gaming, 10 Step Guide for Parents
http://playsmartplaysafe.eu/wp-content/uploads/2011/02/Xbox360SaferFamilyGamingGuide.pdf