Camrose
Early Years Centre for Children & Families

E-Safety/ICT Acceptable Use Policy

This policy is reviewed annually by the Governing Body and was last reviewed on 18.10.2016

E-Safety Lead: Anita Barter

Governor Lead: Rebecca Walker

Contents

Section		Contents	Page(s)
1		Introduction	**3**
2		Why do we have e-Safety and Acceptable Use Policies (AUP)?	**4/5**
3		Scope of the Policy	**4/5**
4		Legal background	**5**
5		Aims	**6**
6		Acceptable use protocol, procedures and sanctions	**6**
	6.1	….Adult responsibilities	**6**
	6.2	….Specific responsibilities	**7/8/9**
	6.3/6.4	….Inappropriate use	**10**
7		Reporting misuse/sanctions	**11**
	7.1	…..Incidents	**11**
	7.2	…..Monitoring	**11**
8		Acceptable Use in practice	**11**
	8.1	….The curriculum	**11/12**
	8.2	….Use of email	**12**
	8.3	….Remote access	**12**
	8.4	….Internet access and filtering	**13**
9		Use of Centre and personal ICT/Technological equipment	**13**
	9.1	….Mobile/smart and other handheld devices	**14**
	9.2	….Laptop/Handheld devices	**14/15**
	9.3	….Removable media	**15**
10		Digital Imagery	**15**
11		Parent/carer Involvement	**16**
12		Use of social networking	**16**
13		Policy Review	**16**
Appendix		1,2,3,4	

1. Introduction

ICT and the Internet have become an integral part of our lives as well as a feature of information finding and of education. It provides our children, staff and parents with opportunities to improve understanding, access online resources and communicate with the world.

The following list identifies common internet-based technologies, which are likely to be used by young people, either at home or in an educational context:

- Websites and the use of apps (on a variety of devices)
- Social Media, including Facebook and Twitter
- Web-enabled mobile/smart phones
- Online gaming
- Learning platforms and Virtual Learning Environments
- Video broadcasting
- Blogs and Wikis
- Email, instant messaging and chat rooms and chat forums

Due to their age the majority of our children are unlikely to have been introduced to most of these applications/services. However, some may already be using them individually, whilst others may have experienced parents/carers or older siblings using them. Hence we cannot be complacent, or assume that the children will not be using technology on a regular basis, and must continue to introduce our children to ICT whilst promoting a safe use of online technologies, in the Centre and at home. Our children will begin to learn how to consider and moderate their own behaviours when using technology and begin to understand how to recognise inappropriate and unsafe behaviour in others.

As some of the technologies listed above will be utilised in the Centre, we recognise that effective policies and clear procedures for safe and appropriate use and education for staff and families about online behaviours, age restrictions and potential risks is absolutely crucial. For our safeguarding to be effective, online safety procedures must be clear, agreed and respected by everyone.

2. Why have an Acceptable Use Policy (AUP)/e-Safety Policy

There are risks associated with the use of on line media, and it is imperative that there are clear rules, procedures and guidelines to minimise those risks when children use these technologies. These risks include:

- Commercial issues with spam and other inappropriate e-mail
- Grooming by people who may abuse children, usually someone pretending to be younger than their true age
- Illegal activities of downloading or copying any copyright materials and file-sharing via the Internet or any mobile device
- Viruses
- Cyber-bullying
- Accessing on-line content, either deliberately or accidentally, which is abusive, offensive or pornographic.

2.1 Duty of care

All schools and nurseries have a duty to ensure that children and young people 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 unlikely that we will be able to eliminate them completely. Any incidents that do arise will be dealt with quickly and according to policy to ensure that the children and staff continue to be protected. The involvement of the children and parent/carers is vital to the successful use of online technologies.

2.2 The purpose of the Acceptable Use Policy

This Acceptable Use Policy sets out the roles, responsibilities and procedures for the safe and appropriate use of all technologies to safeguard the children and adults. The policy recognises the ever changing nature of emerging technologies and highlights the need for regular reviews to incorporate developments within ICT. This policy explains procedures for any unacceptable or misuse of these technologies by adults or children including:

- The steps taken in the Centre to ensure the e-Safety of children when using the internet and other related technologies.
- The Centre's expectations for the behaviour of staff whilst using the internet and related technologies in and out of the Centre.
- The Centre's expectations for the behaviour of staff when using ICT both professionally and socially as well as for accessing and using data.

[1] *The term 'online safety' is to be used to encompass the safe use of all forms of information and communication technologies. The aim, through online safety, should be to reasonably protect all users of such technologies from potential and known risk. Technology and behaviours will be managed.*
[2] *The term 'e-safety' will be used to encompass the safe use of all on-line technologies in order to protect children and adults from potential and known risks.*

3. Scope of the policy

This policy applies to all staff, children, governors, parents, visitors, volunteers and contractors accessing the internet or using technological devices on Centre premises. This includes use of personal devices, such as mobile phones or digital recording equipment including cameras or I-pads which are brought into the Centre. This policy is also applicable where staff or individuals have been provided with Centre devices for use off-site, such as school laptop or work mobile phone. The Centre is expected to ensure that non-employees onsite are made aware of the expectation that technologies and the internet are used safely and appropriately.

3.1 This document comprises the Camrose Centre's Acceptable Use policy, Internet policy, Camera and digital images policy, mobile phone policy and ICT Misuse policy.

3.2 This policy document should be used in conjunction with the following policies:

- Safeguarding and Child Protection policy
- Behaviour policy
- Health and Safety policy
- Technology and ICT policy
- Whistleblowing policy
- Social Networking Policy (Appendix 3)

4. Legal Background

All adults who come into contact with children and young people in their work have a duty of care to safeguard and promote their welfare. The legal obligations and safeguarding duties of Centre employees in relation to use of technologies feature within the following legislative documents which should be referred to for further information:

- The Children Act (2004)
- School Staffing (England) Regulations (2009)
- Working Together to Safeguard Children (2010)
- Education Act (2002)
- Safeguarding Vulnerable Groups Act (2009)
- Keeping Children safe in Education 2016

In addition to this, local procedures can be found at the Northamptonshire Safeguarding Children Board website.

5. Aims

The aims of this policy are to:

- emphasise the need to educate staff, children and parents about the advantages and disadvantages of using new technologies within and outside the Centre.
- provide safeguards and rules for acceptable use to guide all users in their online experiences.
- ensure adults are clear about procedures for misuse of any technologies both within and beyond the Centre, and how to manage breaches of policy in accordance with safer working practices.
- develop links with parents/carers and the wider community ensuring input into policies and procedures with continued awareness of the benefits and the potential issues related to technologies.
- safeguard our children and educate staff and parents by promoting appropriate and acceptable use of information and communication technology (ICT).
- outline the roles and responsibilities of all individuals who are to have access to and/or be users of, work-related ICT systems.
- ensure all ICT users have an acute awareness of risk, a clear understanding of what constitutes misuse and the sanctions that may be applied.

6. Acceptable Use - Protocol, procedures and sanctions

6.1 Adult Responsibilities

All adults (employees or volunteers) have a shared responsibility to ensure that our children are able to use the internet and related technologies appropriately and safely. All adults in the setting are bound to the terms and conditions outlined in this document and a copy of this document is made available to all staff and shared with any volunteers, visitors or contractors.

6.2 Specific Responsibilities

(I). Head of Centre and Governors: The Head and Governors have overall responsibility for e-Safety as part of the wider remit of safeguarding and child protection. To meet these responsibilities, the Head and Governors should:

- Designate an e-Safety Lead to implement agreed policies, procedures, staff training, curriculum requirements and take the lead responsibility for ensuring e-Safety is addressed appropriately. All employees, students and volunteers should be made aware of who holds this post within the Centre.

- Ensure all staff and employees adhere to procedures and protocols outlined in the policies and guidance agreed by Governors.
- Provide a safe, secure and appropriately filtered internet connection for staff, children and families at nursery.
- Provide resources and time for the e-Safety lead and employees to be trained and update protocols where appropriate.
- Promote e-safety awareness across the seven areas of learning as set out in the Early Years Foundation Stage guidance (2012) and have an awareness of how this is being developed, linked with the Centre's development plan.
- Ensure that any equipment which holds sensitive or confidential information and leaves the Centre (e.g. iPads, staff laptops and memory sticks) is encrypted.
- Share any e-safety progress and curriculum updates at all governing body meetings and ensure that all present understand the link to child protection.
- Ensure that e-safety is embedded within all child protection training, guidance and practices.
- Elect an e-Safety Governor to challenge the Centre about e-Safety issues.
- Make employees aware of the NSCB Inter-agency Child Protection procedures at www.northamptonshirescb.org.uk

(II). e-Safety Lead

The nominated e-Safety lead should:

- Recognise the importance of e-Safety and understand the Centre's duty of care for the-Safety of all children and staff.
- Establish and maintain a safe ICT learning environment.
- Ensure that all individuals in a position of trust who access technology with students understand how filtering levels operate and their purpose.
- With the support of the ICT provider, ensure that filtering is set to the correct level for all children and adults accessing the internet.
- Report issues of concern and update the Head on a regular basis.
- Liaise with all members of staff so that procedures are updated and communicated, and take into account any emerging e-safety issues and technological changes.
- Co-ordinate and deliver employee training according to new and emerging technologies so that the correct e-Safety information is being delivered.
- Maintain an e-Safety Incident Log (Appendix 1) to be shared with the Head and Governors at governing body meetings.
- Implement a system of monitoring employee and children use of Centre issued technologies and the internet where appropriate.

(III). Individual Responsibilities

All staff, including volunteers and students under the age of 18, must:

- Take responsibility for their own use of technologies and the internet, making sure that they are used legally, safely and responsibly.
- Ensure that children and young people in their care are protected and supported in their use of technologies so that they can be used in a safe and responsible manner. Children should be informed about what to do in the event of an e-Safety incident.
- Report any e-Safety incident, concern or misuse of technology to the e-safety Lead or Head, including the unacceptable behaviour of other members of the Centre's community.
- Only use the Centre's ICT systems and resources for all Centre related business and communications. Centre issued email addresses, mobile phones and cameras must always be used by employees unless specific written permission to use a personal device has been granted by the Head, for example, for use in an emergency on an educational visit.
- Ensure that all electronic communication with children, parents, carers, employees and others is compatible with their professional role and in line with the Centre's protocols. Personal details, such as mobile number, social network details and personal e-mail should never be shared or used to communicate with children and their families.
- Not post online any text, image, sound or video which could upset or offend any member of the Centre community or be incompatible with their professional role. The Centre's Governing Body requests that staff acknowledge and act on the fact that behaviour in their personal lives may impact upon their work with those children and young people if shared online or via social networking sites.
- Protect their passwords/personal logins and log-off the network wherever possible when leaving work stations unattended.
- Understand that network activity and online communications on Centre equipment (both within and outside the Centre) may be monitored and should only be used for Centre business.
- Understand that employees, who ignore security advice or use email or the internet for inappropriate reasons, risk dismissal and possible police involvement if appropriate.
- Comply with current legislation.

Staff are asked to read and sign our Acceptable Usage/Use of digital technology rules (see Appendix 2).

(IV). ICT Technician

ICT Technician is responsible for ensuring that:

- the Centre's ICT infrastructure is secure and not open to misuse or malicious attack.
- anti-virus software is installed and maintained on all school machines and portable devices.
- the Centre's filtering policy is applied and updated on a regular basis and that responsibility for its implementation is shared with the e Safety Lead and the Designated Safeguarding Lead.
- any problems or faults relating to filtering are reported to Designated Safeguarding Lead and to the broadband provider immediately and recorded on the e Safety Incident Log (Appendix 1).
- users may only access the Centre's network through a rigorously enforced password protection policy, in which passwords are regularly changed.
- 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.
- the use of the Centre network is regularly monitored in order that any deliberate or accidental misuse can be reported to the E Safety Lead.

(V). The Children

All staff recognise that it is important for children to be e-safe from an early age and that the nursery plays a vital role in this. The practitioners in the nursery support the children in using ICT as part of their learning experiences across all areas of the curriculum and believe that, used correctly, ICT will not only raise standards, but will also support practitioners in their work with children. Our internet access is designed expressly for our children and includes appropriate filtering to the age of our children. In line with our other policies that protect children from danger we provide as safe an internet environment as possible. All staff, therefore, must ensure that:

- Children use the internet and ICT technologies safely within the nursery under the direct supervision of a member of staff.
- Children's Internet access is planned to enhance activities that will support their learning.
- Children are helped to understand how to ask for help if they come across materials they may make them feel uncomfortable.
- Websites that are used during nursery sessions are monitored.
- Login passwords are for the expressed use of the staff.
- Children begin to understand, and follow, the children's 'Acceptable Use Rules' (Appendix 2)

6.3 Inappropriate Use - Procedure for following up instances

(I). Staff - In the event of staff misuse, if an employee is believed to have misused the internet or school network in an illegal, inappropriate or abusive manner, a report must be made to the Head of Centre, who is the Designated Safeguarding Lead **immediately**. The appropriate procedures for allegations must be followed and the following teams/authorities contacted:

- LADO (Local Authority Designated Officer)
- Police/CEOP (if appropriate)

Please refer to the e-Safety Incident Flowchart (Appendix1) for further details.

In the event of minor or accidental misuse, internal investigations should be initiated and staff disciplinary procedures followed only if appropriate.

Examples of inappropriate use

- Accepting or requesting children and their parents as 'friends' on social networking sites, or exchanging personal email addresses or mobile phone numbers with children and their parents.
- Behaving in a manner online which would lead any reasonable person to question an individual's suitability to work with children or act as a role model.
- Publishing defamatory and/or false materials about the Camrose Early Years Centre, children, colleagues or other partners on social networking sites.

(II). Children - In the event of inappropriate use by a child, an adult will immediately attempt to minimise or close the content and then take the necessary action.

6.4 Useful Links

NASUWT Social Networking- Guidelines for Members
http://www.nasuwt.org.uk/InformationandAdvice/Professionalissues/SocialNetworking

NUT E-Safety: Protecting School Staff - Guidance for Members
http://www.teachers.org.uk/node/12516

UNISON- Guidance on Social Networking
http://www.unison.org.uk/education/schools/pages_view.asp?did=9786

7 Reporting/Monitoring usage Procedures

7.1 Incident Reporting

In the event of misuse by staff or children, including use of the Centre network in an illegal, unsuitable or abusive manner, a report must be made to the Head/Designated Safeguarding Lead immediately and the e –Safety Incident Flowchart and the Centre's safeguarding procedures will be followed (See appendix 1).

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, Network Manager and Senior Information Risk Owner (SIRO).

All incidents must be recorded on the E-Safety Incident Log (See Appendix 1) to allow for monitoring, auditing and identification of specific concerns or trends.

7.2 Monitoring ICT usage

The Centre's ICT technician will support the Head of Centre, Finance and Business Manager and E-safety lead to monitor and record user activity, including any personal use of the Centre ICT system (both within and outside of the Centre environment) and users are made aware of this in the Acceptable Use Policy.

8. AUP in practice: Procedures and Protocols

The Centre strives to embed e-Safety in all areas of our curriculum and key online safeguarding messages are reinforced wherever possible when ICT is used. The principles and procedures outlined above are embedded into our Curriculum in the following ways**:**

8.1 The Curriculum

- Key online safeguarding messages are reinforced wherever ICT is used with staff and where appropriate in the learning experiences offered to our children.
- The Centre follows the Early Years Foundation Stage and the curriculum guidance for 'Technology' as outlined in the Development Matters Framework document.
- When using ICT if appropriate there are opportunities for informal discussions with the children about online risks and personal protection strategies.
- Parents and staff are signposted to national and local organisations for further support and advice relating to e -safety issues, such as Child line and CEOP (**C**hildhood **E**xploitation and **O**nline **P**rotection Centre)

8.2 Use of email

- The Centre provides some staff with a professional email account to use for all Centre related business, including communications with children, parents and carers. This allows for email content to be monitored and protects staff from the risk of allegations, malicious emails or inappropriate contact with children and their families.
- Staff members are advised not to engage in any personal communications (i.e. via Hotmail or Yahoo accounts) with current or former children/parents. If this should occur they should follow the rules outlined in the AUP and not publish defamatory and/or false materials about the Camrose Early Years Centre, children, colleagues or other partners.
- All emails should be professional in tone and checked carefully before sending, just as an official Centre letter would be.
- Staff should inform their line manager or the e-Safety Lead if they receive an offensive or inappropriate email via the Centre system.
- It is the responsibility of each account holder to keep their password secure and to report any suspected breaches of password security to the e-Safety Lead or Head.
- Account holders must never share their password with another user, or allow access to their email account without the express permission of the e-safety Lead or the Head.

8.3 Managing remote access

As technology continues to develop, schools and their staff are increasingly taking advantage of opportunities for off-site access and email using remote access facilities. For data security and safeguarding purposes, it is crucial that staff are aware of the following restrictions on use:

- Equipment such as laptops should always be packed, stored and secured when offsite e.g. not left in a car overnight.
- Only equipment with the appropriate level of security should be using for remote access (i.e. encryption, passwords on any devices where sensitive data is stored or accessed)
- Log-on IDs and PINs should be confidential and use information that cannot be easily guessed (e.g. date of birth, telephone number, number patterns)

8.4 Internet Access and Age-Appropriate Filtering

Broadband Provider: Schools Broadband

Service Provider: Talk Straight

Children may have opportunities to access supervised safe and secure internet usage as part of the learning experience. The Head is ultimately responsible for ensuring that the Centre 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 Centre has the following filtering measures in place:

- Filtering levels are managed and monitored on behalf of the Centre by Schools Broadband (Open Hive and Fortinet), which ensures that filtered access at the highest levels for all members of staff and children. In addition to the above, the following safeguards are also in place:
- Anti-virus and anti-spyware software is used on all network and standalone PCs of laptops and is updated on a regular basis.
- A firewall ensures that information about children and young people cannot be accessed by unauthorised users.
- The expectations for the online conduct of staff is addressed above staff are required to preview any websites before use, including those which are recommended to, or by, parents.

9 Use of Centre and Personal ICT equipment

A log of all ICT equipment (including serial numbers), is maintained by the Admin Team. With respect to the ICT equipment owned, or used by the Centre:

- Personal or sensitive data is not stored on Centre devices (e.g. laptops, iPads, PC or USB Memory Sticks) unless encryption software is in place. This is true also of any photographs or videos of children.
- All such material should be stored either on the Centre network or on an encrypted device and deleted when no longer required.
- Time locking screensavers are in place on all devices in Centre to prevent unauthorised access, particularly on devices which store personal or sensitive data.
- Personal ICT equipment, such as laptops or memory sticks, must not be connected to the Centre network without explicit consent from the Network Manager and a thorough virus check.

9.1 Mobile/Smart Phones

Staff/Visitor use:

- All staff must ensure that their mobile phones, personal cameras and recording devices are stored securely in their lockers or drawers during working hours or when on outings (This includes visitors, volunteers and students).
- Mobile phones must only be used in the private offices and the staff room the Centre (unless authorised by the Head).

- During Centre outings nominated staff will have access to a Centre mobile/personal phone which can be used for emergency contact purposes.
- It is the responsibility of the adult to ensure that there is no illegal or inappropriate content stored on their device when brought onto Centre grounds.
- Personal mobile phones should never be used to contact children, young people or their families, nor should they be used to take videos or photographs of the children. Centre issued devices **only** should be used in these situations.

9.2 Laptops/Hand-held devices (e.g. iPads/tablets)

- Staff must ensure that all sensitive Centre data is stored on the network (shared drive) and not solely on the laptop or device, unless the device is encrypted. 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.
- Staff are aware that all activities carried out on Centre devices and systems, both within and outside of the Centre environment, will be monitored in accordance with this policy.

9.3 Removable Media (Memory Sticks/USB)

- Where staff may require removable media to store or access sensitive data (e.g. pupil attainment and assessment data) off site, only encrypted memory sticks will be used.
- Any passwords used for encrypted memory sticks/or other devices will be remain confidential to the user and shared only with authorised IT personnel for security and monitoring purposes.

10 Photographs and Videos

Digital photographs and videos are an important part of the learning experience for our children. We recognise our responsibility to ensure that our children learn about the safe and appropriate use of digital imagery, and that our staff model good practice. To this end, there are strict policies and procedures for staff, children and parents about the use of digital imagery within the Centre.

- Written consent will be obtained from parents or carers before photographs or videos of young people are taken or used within the Centre environment, including the Centre website or associated marketing material
- Staff are not permitted to use personal devices, such as cameras, video equipment or camera phones, to take photographs or videos of children.

- Permission will be sought from any child or 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.
- Images will never show children in inappropriate clothing.
- Digitised images will be deleted from devices immediately after they have been used. Unused photographs will be destroyed (shredded) or returned directly to parents.
- Staff will ensure that parents/visitors do not use mobile phones or other hand-held devices in the Centre.
- Parents are requested not to use their mobile devices or any photographic equipment on Centre premises.

11 Parent/Carer Involvement

As part of the Centres commitment to developing e-Safety awareness amongst children and young people, every effort is made to engage parents and carers in the process.

- All parents/carers will be made aware of our 'Technology Rules' (see Appendix 2).
- E-Safety information will be provided to carers to help raise awareness of key internet safety issues and highlight safeguarding measures in place within the Centre.

12 Use of Social Networking Sites

Staff and parents are advised against the misuse of network sites such as Facebook to share confidential or potentially negative or abusive comments regarding the Centre, a member of staff, parent or child. All staff have seen and are expected to follow the NCC document 'Use of social networking – a guide for professional working with young people (Appendix 3).

13 Policy Review

The e-Safety/ICT Acceptable Use Policy will be updated to reflect any technological developments and changes to the Centre's ICT Infrastructure.