Reviewed February 2017

SHIRLEY COMMUNITY NURSERY AND PRIMARY SCHOOL - E-SAFETY POLICY

E-safety Policy: Safeguarding our children

Background to the Policy

The purpose of this policy is to describe the safeguarding measures in place for adults and children in school:

- the ground rules we have developed in school for using the Internet, online technologies and handheld devices
- how these fit into the wider context of our other school policies
- the methods used to protect children from sites containing pornography, racist or politically extreme views and violence

Ultimately, the responsibility for setting and conveying the standards that children are expected to follow when using technology, media and information resources, is one the school shares with parents and carers. At Shirley Community Nursery and Primary School, we feel that the most successful approach lies in a combination of site filtering, of supervision and by fostering a responsible attitude in our pupils in partnership with parents/carers.

This policy (for all staff, governors, visitors and pupils) is inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, personal digital assistants (PDAs), tablets, webcams, whiteboards, digital video equipment etc). Technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc), should also follow the same guidance.

The development of our safety policy involved:

- The Headteacher
- Designated CP person
- ICT Subject Leader
- PSHE subject leader
- Safeguarding Governor
- School council representatives
- Prevent designated person

It was reviewed in February 2017 presented to the Governing body on 13 July 2017

It will be available:

- On the school website
- Via the office
- On the school server

Signature of the Chair of the Governing Body

……

SHIRLEY COMMUNITY NURSERY AND PRIMARY SCHOOL - E-SAFETY POLICY

Rationale

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, our school needs to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

The school's responsibility

At Shirley Community Nursery and Primary School, we understand the responsibility to educate our pupils and staff on e-safety issues; ***teaching them the appropriate behaviours*** and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

While children and young people need support to keep them safe online, the risks associated with the use of technology are not restricted to just them. E-Safety issues can also affect adults who work or are associated with the school. For example, school and personal data being entered on web/social networking sites, fraudulent email traps and cyberbullying. It is impossible to eliminate risk completely. It is therefore essential, through good educational provision to manage the risk and deal with any threat to safety.

What is ICT?

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently, the internet technologies children and young people are using both inside and outside of the classroom include:

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

The risks

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

The use of these exciting and innovative technology tools in school and at home has been shown to raise educational standards and promote pupil achievement. Yet at the same time we recognise that the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet
- PREVENT
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

CPD

All staff are given training on e-safety and The Prevent Duty as part of their induction to the school. This forms part of their safeguarding training.

Teaching and Learning Using Online Technologies

The internet is a part of everyday life for education, business and social interaction.
Benefits of using online technologies in education include:

- Access to world-wide educational resources
- Inclusion in the NEN (National Education Network) connecting all UK schools and resources
- Access to experts who would otherwise be unavailable
- Access to anytime, anywhere learning
- Collaboration across schools, networks of schools and services

Curriculum

When using online technologies, it is essential that children understand how to behave in a safe and responsible manner and also how to react when faced with inappropriate content or situations which make them feel uncomfortable.

At Shirley Community Nursery and Primary School, we teach online safety through our computing and PSHE curriculum and refer to it in all that we do when using technology. We believe that a comprehensive programme of e-safety education is vital for developing our pupils' ability to use technologies safely. As well as holding an 'e-safety day' each year, we achieve pupils' safe use of technology by using a combination of discrete and embedded activities drawn from a selection of appropriate materials (see *appendix 1 – Progression materials for e-safety)*.

Our programme for e-safety education is evidenced in teachers' planning either as discrete or embedded activities. This is monitored by the ICT/Computing subject leader. Members of staff constantly monitor pupils' use of the internet and other technologies and are able to monitor pupils' use of Starz communication and publishing tools.
Messages involving risks and rules and responsibilities are taught and/or reinforced as detailed in the school's AUP (see *appendix 2 – Acceptable Use Policy*).

Technology in our School

The school's ICT infrastructure is designed to minimise the risks associated with adult and pupil use of technology. This is provided and maintained by both E2BN and the Local Authority's Education ICT Service.

E2BN's Protex web filtering system received full Becta accreditation in 2007 by blocking over 90% of all inappropriate material. E2BN also manage a distributed caching service which is integrated with the web filtering service.

E2BN's Website

This helps to ensure that staff and pupils rarely encounter material which is inappropriate or offensive. If / when they do, the school's AUP and e-safety education programme ensure that they are equipped to deal with any issues in the most appropriate way.

Whilst we recognise the benefits of individual pupil logins to our school network, we prefer to use year group logins for ease of access. All members of staff have individual, password protected logins to the school network and visitors to the school can access part of the network using a generic visitor login and password.

The school's network can either be accessed using a wired or wireless connection. However, the wireless network is encrypted to the standards advised by the Local Authority and the wireless key is kept securely by the school office. School staff and pupils are **not** permitted to connect personal devices to the school's wireless network.

Safeguarding Our Children Online

Shirley Community Nursery and Primary School recognises that different users will be expected to use the school's technology systems in different ways – appropriate to their age or role in school. We acknowledge the need to:

Equip children to deal with exposure to harmful and inappropriate content and contact, and equip parents to help their children deal with these things and parent effectively around incidences of harmful and inappropriate conduct by their children.

UKCCIS – June 2008

The school has published an Acceptable Use Policy for pupils and staff who sign to indicate their acceptance of our AUP and relevant sanctions which will be applied should rules be broken.

Any known or suspicious online misuse or problem will be reported to the designated E-Safety Co-ordinator for investigation/ action/ consequences or the headteacher. The school will keep evidence and/or contribute to a log of any 'extreme' or 'unusual' actions that a pupil has been involved in online. This log will be used to keep track of the child's behaviours over the entire time they are at the school and will be stored alongside other incident logs. These are stored securely by the head teacher (see *appendix 4 – logging an e-safety concern about a child).*

Responding to Incidents

It is important that all members of staff, teaching and non-teaching, are aware of how to respond if an e-safety incident occurs or they suspect a child is at risk through their use of technology. Responding to an e-safety incident in school, is no different to responding to other incidents in school.

If an e-safety incident occurs, Shirley Community Nursery and Primary will follow its usual procedures for dealing with other incidents including internal sanctions and involvement of parents (for ICT, this may include the deactivation of accounts or restricted access to systems as per the school's AUP). Where the school suspects that an incident may constitute a Child Protection issue, the usual Child Protection procedures will be followed.

Any concerns about children relating to radicalisation and extremism will be reported to the Prevent Lead.

Dealing with Incidents and Seeking Help

If a concern is raised, staff will refer immediately to the designated persons for child protection. If that is not possible, refer to the team leader or, if necessary, the Chair of Governors.
It is their responsibility to:
Step 1: Identify who is involved – any combination of child victim, child instigator, staff victim, or staff instigator.
Step 2: Establish the kind of activity involved and whether it is illegal or inappropriate. If you are in doubt consult the Education Child Protection Service helpline - 0345 0455203.
Step 3: Ensure that the incident is documented using the standard child protection incident logging form
Step 4: save any evidence if available
Step 5: the designated person will decide if the concern is recorded on a form for logging a concern about a child's safety and welfare or an e-safety concerns form *Appendix 3: logging an e-safety concern about a child.*

Depending on the judgements made at steps 1 and 2, the following actions should be taken
Staff instigator – follow the standard procedures for Managing Allegations against a member of staff. If unsure seek advice from the Local Authority Designated Officer or Education Officer.
Staff victim – Seek advice from your HR provider and/or Educational Child Protection Service.
Illegal activity involving a child – refer directly to Cambridgeshire Constabulary – 0845 456 4564 – make clear that it is a child protection issue.
Inappropriate activity involving a child – follow standard child protection procedures. If unsure seek advice from Education Child Protection Service helpline: 0345 0455203 (up to date numbers are always kept in the school office).

Minimising risk

At Shirley Community Nursery and Primary School, we carry out generic risk assessments for the use of technologies and share these with the relevant groups e.g. staff, pupils and parents. Examples can be seen in appendix 4- risk assessment example.

Links to other documents

Several documents are referred to within this policy. This section outlines specific sections that link to e-safety.

Safer Working Practice for those working with children and young people in education settings (October 2015):

11. Social contact outside of the workplace

It is acknowledged that staff may have genuine friendships and social contact with parents of pupils, independent of the professional relationship. Staff should, however, also be aware that professionals who sexually harm children often seek to establish relationships and contact outside of the workplace with both the child and their parents, in order to 'groom' the adult and the child and/or create opportunities for sexual abuse.

It is also important to recognise that social contact may provide opportunities for other types of grooming such as for the purpose of sexual exploitation or radicalisation. Staff should recognise that some types of social contact with pupils or their families could be perceived as harmful or exerting inappropriate influence on children, and may bring the setting into disrepute (e.g. attending a political protest, circulating propaganda).
If a pupil or parent seeks to establish social contact, or if this occurs coincidentally, the member of staff should exercise her/his professional judgement. This also applies to social contacts made through outside interests or the staff member's own family.
Some staff may, as part of their professional role, be required to support a parent or carer. If that person comes to depend upon the staff member or seeks support outside of their professional role this should be discussed with senior management and where necessary referrals made to the appropriate support agency.

12. Communication with children (including the use of technology)

In order to make best use of the many educational and social benefits of new and emerging technologies, pupils need opportunities to use and explore the digital world. E-safety risks are posed more by behaviours and values than the technology itself.
Staff should ensure that they establish safe and responsible online behaviours, working to local and national guidelines and acceptable use policies which detail how new and emerging technologies may be used.

Communication with children both in the 'real' world and through web based and telecommunication interactions should take place within explicit professional boundaries. This includes the use of computers, tablets, phones, texts, e-mails, instant messages, social media such as Facebook and Twitter, chat-rooms, forums, blogs, websites, gaming sites, digital cameras, videos, web-cams and other hand held devices. (Given the ever changing world of technology it should be noted that this list gives examples only and is not exhaustive.)

Staff should not request or respond to any personal information from children other than which may be necessary in their professional role. They should ensure that their communications are open and transparent and avoid any communication which could be interpreted as 'grooming behaviour'

Staff should not give their personal contact details to children for example, e-mail address, home or mobile telephone numbers, details of web based identities. If children locate these by any other means and attempt to contact or correspond with the staff member, the adult should not respond and must report the matter to their manager. The child should be firmly and politely informed that this is not acceptable.

Staff should adhere to their establishment's policies, including those with regard to communication with parents and carers and the information they share when using the internet.

The school uses the above guidance and agrees that:

The school

- Has in place an Acceptable Use Policy
- Continually self-reviews the e-safety policy in the light of new technologies
- Ensures that staff are aware of e-safety through training and issuing of policies

Adults

- Ensure that personal social networking sites are set at private and pupils are never listed as approved contacts
- Never use or access social networking sites of pupils
- Not give their personal contact details to pupils, including their mobile telephone number
- Only use equipment provided by school to communicate with children, making sure that parents have given permission for this form of communication to be used
- Only make contact with children for professional reasons
- Recognise that text messaging should only be used as part of an agreed protocol and when other forms of communication are not possible
- Not use internet or web-based communication channels to send personal messages to a child

Guidance on the use of **mobile phones and cameras** is included in our policy (appendix 8).

Terms used in this policy
AUP: Acceptable Use Policy.
A document detailing the way in which new or emerging technologies may/may not be used – may also list sanctions for misuse.
Child: Where we use the term 'child' (or its derivatives), we mean 'child or young person'; that is anyone who has not yet reached their eighteenth birthday.
E-safety: We use e-safety, and related terms such as 'online', 'communication technologies', and 'digital technologies' to refer to all fixed and mobile technologies that children may encounter, now and in the future, which might pose e-safety risks. We try to avoid using the term 'ICT' when talking about e-safety as this implies that it is a technical issue – which is not the case. The primary focus of e-safety is child protection: the issues should never be passed solely to technical staff to address.
Safeguarding: Safeguarding is defined (for the purposes of this document) as the process of increasing resilience to risks when using technology through a combined approach to policies and procedures, infrastructure and education, underpinned by standards and inspection. E-safety is just

one aspect of a much wider safeguarding agenda within the UK, under the banner of *Every Child Matters: Change for Children*. Those with responsibility for the development and delivery of e-safety policies should embed their work within the wider safeguarding agenda, and work across services to ensure that they are delivering the best possible opportunities for the children and young people in their care.
Users: We use this term, and related terms such as service users and end users, to mean those people who will ultimately be bound by the provisions of an AUP.
AUP – this is for pupils, staff, parents and carers, or members of the wider community, depending on provisions of our AUP or the context in which we operate.

Appendices:

- Appendix 1: Progression planning for e-safety (Cambridgeshire ICT service)
- Appendix 2: Acceptable Use Policy
- Appendix 3: logging an e-safety concern about a child
- Appendix 4: Risk assessment example
- Appendix 5: Policy for the use of mobile phones and cameras (2015)

Staff will sign to confirm that they have read and understood this policy.