E-Safety & ICT Acceptable Use Policy

Dee Point Primary School

Delegate Function: Headteacher & SLT
Approved by Governors: March 2016
Updated: February 2016
Review date: March 2017

This policy/document was reviewed by:-

Signed…… Date:

Position……

Signed…… Date:

Position……

The next revision date is: ……

Aims

One of the main aims of Dee Point is that every member of the community feels safe. As a result this policy must be read in conjunction with all other Safeguarding & Child Protection Policies.

We aim that every member of the school community feels safe and secure using ICT and different technologies at home and at school.

We also aim to educate children and parents in how to use ICT safely and appropriately. Primarily we will be looking at the internet, but we will also look at other communication tools such as mobile phones. We will highlight both the benefits and risks of using such technologies and provide safeguards as well as awareness so users can control their online experiences.

The Computing Lead and Designated Teacher for Safeguarding (Angela Livingstone and Dave Williams) will stay abreast of the most up to date E-Safety and Internet Safety policies and practice.

Teaching and Learning

The internet is a vital part of everyday life from education to business. Consequently, it is imperative that school provide children with quality internet access. The internet is a statutory part of the school curriculum and we particularly link this to our Virtual Learning Platform.

- The schools internet is filtered appropriately in comparison to the age of our pupils.
- We have the authority to choose which websites are accessible at school.
- The pupils are taught how to use the internet acceptably and are given learning objectives so they know exactly what is expected from them. Pupils are taught how to effectively use search engines to research the internet and are directed towards using the BBC search engines because all their pages have been vetted. In addition to this, pupils are taught how to evaluate the internet content by validating information before accepting its accuracy.
- Any inappropriate websites accessed are passed onto our ICT support (Dave Simpson or Ellen Hope) who have the ability to block the website. They will also inform the Council's technical service team.
- The school will ensure that the materials used by staff and pupils comply with law.
- All staff will sign the 'Acceptable use agreement and code of conduct.' ***(Appendix 2)***

The schools ICT systems capacity and security will be reviewed regularly by following the following steps:-

- Virus protection will be updated regularly by Dave Simpson (ICT Support)
- Security strategies will be discussed with the Cheshire West and Chester Authority, Cosocius and Internet Service Provider.

E-safety Curriculum

- All year groups from Nursery to Year 6 will have an e safety scheme of work.
- This scheme of work runs alongside the computing curriculum and the SRE/PSHE curriculums.
- Teachers will teach the E safety scheme of work over a half term or term (it is up to the teacher's discretion, when best to teach the scheme).

Virtual Learning Platform

The aim of the VLP is to give children, parents, governors and members of the community up to date information about the school. It is also seen as one of the first points of call for prospective parents and as such, needs to maintain the friendly, welcoming feel that Dee Point presents.

Our Virtual Learning Platform will …

- Provide information to our parents through the school website such as newsletters, general letters and dates.
- Provide contact details on the VLP such as the school address, email, telephone number and map. No staff or pupils personal information will be published.
- Be in line with the current Government expectations for a school website. *What maintained schools must publish online (18th September 2015)*
- Promote safe use of the internet
- Provide governors access to documentation and a secure area so communication can be regular, private and aid in the schools development.

VLP Management

- The Head teacher, Chair of Governors, Computing Leads and ICT support will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Written permission from parents/carers will be obtained before photographs of pupils are published on the school website.
- All photos will be re sized to the smallest pixel size before being up loaded onto the internet.
- This permission form will allow teachers and members of staff to publish the children's work.
- No names of children will be used on the public facing pages of the website but some photographs will be used (Similarly to the School Prospectus).
- All adults will be able to update every page.
- Computing support (E.Hope) will manage users, ensuring that users have a username and secure password and are allocated to appropriate areas.
- Managing the layout of the Learning Platform.
- CPD for relevant staff will be up to date, in line with the schools CPD, Monitoring and Evaluation Schedule.

Social Networking

- The school will manage all access to social media sites.
- Pupils will be instructed not to give out personal details which may identify them or their location. (Part of the E safety schemes of work)
- Pupils and parents will be advised that the use of social network spaces for pupils is inappropriate, specifically Facebook, as a result of Local Authority Advice.

Twitter

- The school currently has a Twitter page (@DeePointPrimary)
- All teachers and key teaching assistants have the password to update the twitter account.
- All tweets are public.
- Photos will be public on the account. All parents have the option to opt out of this when their child begins school in Reception.
- Only reputable Twitter accounts will be followed.
- No parent or pupil accounts will be followed by Dee Point Primary School.

E – Cadets

- The school currently operates an effective E-cadet program with 8 children across Key Stage 2 who are elected for a year to undertake a range of ICT awareness programs as identified in the school's SSDP. These include:
    - Communications on line
    - Data Protection
    - Parental knowledge and understanding

Managing Emerging Technologies

- New and emerging technologies will be examined for both educational benefit and risk assessment.
- Staff will contact the school office when a message needs to be sent home to parents.
- In emergency situations, staff may be required to use their personal phone to contact emergency services or parents. When contacting parents, staff will use 141 to keep their own mobile phone number private.
- When contacting parents, Group Call (a SMS messaging service) may sometimes be used to send a message to multiple recipients.

Protecting Personal Data

- Personal Data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- Staff may save work, planning and assessment information on a USB or external hard drive to access at home. Any sensitive or personal data, must be securely stored either on an encrypted device, or in a password protected folder. Staff will sign the 'Acceptable use agreement and code of conduct.'

Staff Email

- All staff have a personal email account. _____@deepointprimary.cheshire.sch.uk
- All staff use this account for business use only.
- All staff remain professional at all times through this form of communication.
- If communications about a child are sent through email, initials must be used, so the child is not easily identified.
- All staff will sign the 'Acceptable use agreement and code of conduct.'

Pupil Email

- Pupils currently do not have a personal school email account.
- Pupils may access an email account that is created by their class teacher in order to teach the email area of the curriculum. This account is closely managed by the teacher and the class teacher is responsible for closing the account after use.
- Pupils must immediately tell a teacher if they receive an offensive or inappropriate email.
- Pupils must not reveal personal details of themselves or others in email, messenger or VLP communication.
- Pupils must not arrange to meet anyone without specific permission.

Internet Access

- KS1 pupils will access the internet through adult led activities. They will be able to access specified internet sites such as Espresso or via hyperlinks.
- KS2 pupils will access the internet during ICT lessons as well as cross curricular lessons.
- All adults will sign the 'Acceptable use agreement and code of conduct.' before using any school ICT resource. A copy of these agreements will be kept by the Computing Lead.
- Any misuse of the VLP or internet access will lead to immediate internet access withdrawal by the Computing Lead.
- The school will take all reasonable precautions to ensure that users access only appropriate materials. If this is the case, children will leave the site immediately and staff will add the website to the inappropriate websites list.

E-Safety Complaints

- Complaints of internet misuse will be dealt with by the Senior Leadership Team.
- Any complaint of staff misuse must be referred to the Head teacher.
- Complaints of a child protection nature must be dealt with in accordance with child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Dee Point will follow the Cheshire West and Chester procedures for dealing with significant incidents.

E-Safety Communication

- E-Safety rules will be posted in the ICT suite and will be discussed with all pupils through the e safety scheme of work.
- Pupils, Staff and Governors will be aware that internet and VLP usage will be monitored.
- Staff will be informed that the E-Safety Policy will be stored in staff share and staff must read it and adopt it.
- Parents will be directed towards the E-Safety policy in newsletters and via the VLP.

Failure to Comply

- Failure to comply with this policy will be investigated by a member of the Senior Leadership Team in line with the Acceptable Use Policy adopted from Cheshire West and Chester (***Appendix 1)***

Appendix 1

(Please refer to Cheshire West and Chester's Acceptable Use Policy)

Appendix 2

Staff Acceptable Use Agreement and Code of Conduct

Date Created: March 2016
Date for Review: March 2017

This has been written after detailed discussions with the local authority advisors for ICT and safeguarding. Everything within this code of conduct is set out for the benefit of the school community as a whole. This policy is be reviewed yearly and adapted as necessary in accordance to relevant documentation.

Use of Facilities

All uses, whether for private or school purposes, in or outside of the work place must observe:-

1. The law.
2. Terms of employment.
3. Financial regulations and codes of practice on financial management.
4. The governor approved ICT/ e-safety policies.

It is not acceptable to use any school or home equipment for the following contexts:

- Illegal activity including links to Radicalisation & Extremism
- Activities for private gain.
- Political comment or campaigning.
- Actions that could embarrass the school or local authority.
- No member of staff can use the school's Wi-Fi system unless in exceptional circumstances agreed with the Headteacher.

The above conditions are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices, webcams, whiteboards, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones and other mobile devices).

Data Protection

You must ensure you:

- Protect personal information or both pupils and staff and adhere to the Data Protection Act (1998).
- Do not disclose any passwords and ensure that personal data (such as data held on SIMS software) is kept secure and used appropriately
- Any data that is stored on a school laptop is password protected, either individual files or whole computer.
- Encrypt any portable storage devices which contain personal information about pupils or staff.
- Do not send any personal information about pupils or staff on other forms of media (social networking sites) apart from school email addresses.

Social Networking Sites

It is **not** acceptable to:-

- Be a friend with any current pupils
- Be friends with any former pupils
- Be friends with parents of pupils
- Make any comment positive or negative regarding school or the local community on any social networking platform
- Message pupils and parents of pupils (text or image) using social media sites
- Upload any images of pupils from a personal media device which are not on school authorised media platforms

- ✳ Upload content (image, text, video or sound) which may upset or offend any member of the whole school community or be incompatible with your professional role
- ✳ Browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory

You **must** ensure you:

- ✳ Have the most secure privacy settings on all social media platforms
- ✳ Communicate with parents using your school email address only

Twitter

- ✳ You must ensure you use only school resources to take pictures of pupils or staff
- ✳ Use only the schools twitter account to upload content related to pupils' and staff
- ✳ Any other tweets or retweets must either:
    - Celebrate achievements / successes across the school
    - Or have an explicit link to educational initiatives / developments / activities.

If at any time you need to report incidents regarding misconduct of this policy or incidents which inadvertently misuse this policy, they must be reported to the computing co-ordinator, e-safety co-ordinator or child protection officers.

Full Name:

Position:

Date:

Signature:

Dee Point Primary School
Approved by Governors: March 2016
Updated: February 2016
Review date: March 2017

This policy/document was reviewed by:-

Signed……

Date:

Position…….

Signed……

Date:

Position…….

The next revision date is: …….