ASHMORE PARK

AND

PHOENIX NURSERY SCHOOLS FEDERATION

DIGITAL SAFEGUARDING POLICY

Compliance Link Governor(s) Review Date	- March 2018
Governing Board Approved/Adopted	- Wednesday 21 March 2018
Policy Review Date	- March 2019

The Federations vision

Both Ashmore Park Nursery and Phoenix Nursery embraces the challenge that technology is considered to be an essential part of modern life and they recognise that it is their duty to provide children with quality technology as part of their learning, this is aimed at their own personal developmental ability.

This policy considers the use of both the fixed and mobile devices with an appropriate internet connection e.g. iPads, PCs, laptops, webcams, digital video equipment, mobile phones, camera phones, personal digital assistants, gaming devices and portable media players. It will be revised to incorporate new and emerging technologies as they appear.

The policy sets out how we protect the interest and safety of the whole school community, integrate ICT across all areas of learning in the Early Years Foundation Stage (EYFS) promoting enjoyment, a personal sense of fulfillment, achievement and the life skills that will help our children thrive in the 21st Century.

- To give children the confidence to use a variety of ICT equipment
- To enable children to use ICT for a variety of purposes
- To help children to become aware of the technology around them in their school, home and local environment.

Equality and inclusion

The use of technology is a part of the statutory curriculum and a necessary means of delivering 21st Century teaching and learning for staff, and children. Internet access is an entitlement for all. However, responsible and **safe use must be at its core**.

Technology in a changing world

Schools are part of a world where technology is integral to the way life is led in the 21st Century. When compared to even 5 years ago the technology available outside school is rapidly increasing. In line with the Gilbert review document ***2020 Vision***, schools need to increasingly respond to:

- An ethnically and socially diverse society
- Far greater access and reliance on technology as a means of conducting daily interactions and transactions
- A knowledge based economy
- Demanding employers, who are clear about the skills their businesses need and value
- Complex pathways through education and training, requiring young people to make choices and reach decisions.

Why do we need to be safe working with technology?

As the uses of online technological resources have grown, so has the awareness of risks and potential dangers that arise for their use. The Federation aims to prepare its learners to be able to thrive and survive in this complex digital world. This policy outlines the safeguarding approach to achieve this.

Management of Digital Safeguarding

Clearly stated roles and responsibilities –

The Headteacher

The Headteacher will ensure that the Digital Safeguarding Policy is implemented, compliance with the policy monitored and that the appropriate roles (see this section), and responsibilities of each School's digital safeguarding structure is in place. The Headteacher will also

- Ensure adequate technical support is in place to maintain a secure ICT system
- Ensure policies and procedures are in place to ensure the integrity of each School's information and data assets
- Ensure liaison with Governors
- Ensure that all staff agree to the 'Acceptable Use Policy for Staff and Senior Students' (See Appendix 1), and that new staff have eSafety included as part of their induction procedures
- Make appropriate resources, training and support available to all members of the school community to ensure they are able to carry out their roles effectively with regard to eSafety
- Receive and regularly review eSafety incident logs; ensure that the correct procedures are followed should an eSafety incident occur in School and review incidents to see if further action is required
- Promote an awareness and commitment to eSafety throughout both Schools
- Be the first point of contact on all eSafety matters
- Lead the Federations eSafety team
- Create and maintain eSafety policies and procedures
- Develop an understanding of current eSafety issues, guidance and appropriate legislation
- Ensure delivery of an appropriate level of training in eSafety issues
- Ensure that eSafety education is embedded across the curriculum
- Ensure that eSafety is promoted to parents and carers
- Ensure that any person who is not a member of school staff, who makes use of the school ICT equipment in any context, is made aware of the 'Acceptable Use Policy for Staff and Senior Students'.
- Liaise with the Local Authority (LA), the Wolverhampton Safeguarding Children's Board and other relevant agencies as appropriate
- Ensure that staff and pupils know the procedure to follow should they encounter any material or communication that makes them feel uncomfortable.

Responsibilities of the Governing Board

That the Safeguarding Link Governor liaises with the Headteacher; monitors practices and reports to the full Governing Board as and when appropriate.

- Read, understand, contribute to and help promote the Federation's eSafety policies and guidance as part of each school's overarching safeguarding procedures
- Ensure appropriate funding and resources are available for each school to implement their eSafety strategy.

Staff eSafety Responsibilities

- Read, understand and help promote the Federation's eSafety policies and guidance
- Read, understand and adhere to the staff 'Acceptable Use Policy for Staff and Senior Students'
- Take responsibility for ensuring the safety of sensitive school data and information
- Develop and maintain an awareness of current eSafety issues and legislation and guidance relevant to their work
- Maintain a professional level of conduct in their personal use of technology at all times
- Embed eSafety messages in learning activities where appropriate
- Supervise children carefully when engaged in learning activities involving technology
- Report all eSafety incidents which occur in the appropriate log and/or report to the Headteacher
- Respect the feelings, rights, values and intellectual property of others in their use of technology, in schools and at home.

Responsibilities of the Parent/Carer

- Help and support their school in promoting eSafety
- Show an interest in how their children are using technology, encourage them to behave safely and responsibly when using technology
- Consult with their School if they have any concerns about their child's use of technology.

Procedures

Any incidents where Staff do not follow the 'Acceptable Use Policy for Staff and Senior Students' will be dealt with following the Federation's normal behavior or disciplinary procedures.

In situations where a member of staff is made aware of a serious eSafety incident, concerning pupils or staff, they will inform the Headteacher who will then respond in the most appropriate manner.

(Please see the Federations Whistle Blowing Policy)

Incidents which create a risk to the security of either school network, or create an information security risk, will be referred to the School's eSafety co-coordinator and technical support, appropriate advice shall be sought, action will be taken to minimise the risk and prevent further instances occurring, including reviewing any policies, procedures or guidance. If the action breaches the Federation's policy, appropriate sanctions will be applied. The Federation will decide if parents need to be informed if there is a risk that children's data has been lost.

The Federation reserves the right to monitor equipment on their premises and to search any technology equipment, including personal equipment with permission, when a breach of this policy is suspected.

Dealing with a Child Protection issue arising from the use of Technology

If an incident occurs, which raises concerns about 'Child Protection' or the discovery of indecent images on the computer, then the procedure outlined in the Wolverhampton Safeguarding Procedures and Guidance will be followed.

Risks and Acceptable Behaviors

General use of the internet - Children will only access the internet when a supervising adult is nearby, please note that there is a filtering system in place across the Federation.

We provide the internet to

- Support curriculum development in all areas of learning
- Support the professional work of staff as an essential professional tool
- Enhance each school's management of information and business administration systems
- Enable electronic communication, the exchange of curriculum and administration data with the LA.

Users are made aware that they must take responsibility of their use of, and their behavior whilst using, their school's ICT systems or a laptop, or device which has been provided by their School and that such activity can be monitored, and checked.

All users of their School ICT or electronic equipment will be required to abide by the relevant 'Acceptable Use Policy for Staff and Senior Students' at all times, whether working in a supervised activity or working independently.

Password/Personal Details

- Staff should abide by the statement in the 'Acceptable Use Policy for Staff and Senior Students' (Appendix 1). It is good practice to change passwords periodically for data security.

Data Security

The Federation recognises their obligation to safeguard staff and children's personal data including that which is stored and transmitted electronically. As a result they regularly review the practices and procedures to ensure that they meet the basic obligation.

Each School is a registered Data Controller under the Data Protection Act 1998 and complies at all times with the requirements of that registration.

Suitable procedures and where necessary, training, are in place to ensure the security of such data including the following:

- All computers or laptops holding sensitive information are set up with strong passwords, have password protected screen savers and screens are locked when they are left unattended
- Staff are provided with appropriate levels of access to their School's management information systems holding pupil data. Passwords are not shared and administrator passwords are kept securely
- Staff are aware of their obligation to keep sensitive data secure when working on computers outside school
- We follow Wolverhampton Local Authority procedures for transmitting data securely
- Remote access to computers is by authorised personnel only
- We have full back up and recovery procedures in place for both School's data
- Where sensitive staff or children data is shared with other people who have a right to see the information, e.g. Governors or the School Improvement Partner (SIP), we label the material appropriately to the remind them of their duty to keep it secure and securely destroy any spare copies.

E-mail

Email is regarded as an essential means of communication. Communication by email between staff, pupils and parents will only be made using either School's email account. All communication should be professional, and related to school matters only. Email messages on school business should reflect a suitable tone and content, and should ensure that the good name of each School is maintained.

Use of both school's email systems is monitored and checked.

School Website

- Each School maintains editorial responsibility for any school initiated website content to ensure that the content is accurate and the quality of presentation is maintained. Each School maintains the integrity of the school website by ensuring that responsibility for uploading material is always moderated and passwords are protected
- The point of contact on the web site is the respective school address, e-mail and telephone number

- Identities of pupils are protected at all times. Photographs of identifiable individual pupils are not published on the website unless the respective School obtains written permission from parents for the use of pupil's photographs. Group's photographs do not have a name list attached

- Staff are encouraged to adopt similar safe and responsible behaviors in their personal use of blogs, wikis, social networking sites and other online publishing outside their school as they are in school

- Materials published by pupils, Governors and staff in a social context, which is considered to bring their school into disrepute or considered harmful to, or harassment of, or member of the school community will be considered a breach of school discipline and treated accordingly.

Managing and Safeguarding ICT Systems

- Each School will ensure that access to their school ICT system is as safe and secure as reasonably possible

- Servers and key hardware or infrastructure is located securely with only appropriate staff permitted access. Servers, workstations and other hardware and software are kept updated as appropriate. A firewall is maintained and virus protection is installed on all appropriate hardware and is kept active and up-to date. Staff have virus protection installed on all laptops used for school activity

- Any administrator or master passwords for school ICT systems are kept secure and available to at least two members of staff e.g. Headteacher and Senior Administrator

- The wireless network is protected by a secure log-on which prevents unauthorised access. New users can only be given access by named individuals e.g. a member of technical support

- We do not allow anyone except technical staff to download and install software onto the network. Staff are allowed administrator rights to download software on school provided laptops only.

Filtering Internet Access

- Web filtering of internet content is provided by Wolverhampton Local Authority. This ensures that all reasonable precautions are taken to prevent access to inappropriate material. It is not, however, possible to guarantee that access to unsuitable material will never occur. Teachers are encouraged to check out websites they wish to use prior to their use. All users are informed about the action they should take if inappropriate material is accessed or discovered on the computer

- Each School decides which users should and should not have internet access, the appropriate level of access, and the level of supervision they should receive. There are robust systems in place for managing the network account and passwords, including safeguarding administrator passwords. Suitable arrangements are in place for visitors to either School who may be granted a temporary log in

- All users are provided with a log in appropriate to their key stage or role in school
- Staff are given appropriate guidance on managing access to laptops which are used both at home and school, and in creating secure passwords
- Access to personal, private or sensitive information is restricted to authorised users only, with proper procedures being followed for authorising and protecting login, and password information.

Mobile phones/technology

- We recognise that many aspects of the curriculum can be enhanced by the use of multi-media and that there are now a wide, and growing range of devices on which this can be accomplished
- Digital images, video and sound recordings are only taken with the permission of participants, images and videos are of appropriate activities, and are only taken of children wearing appropriate dress. Full names of participants are not used either within the resource itself, within the file name or in accompanying text online
- All parents and visitors are asked not to use mobile phones when in their Nursery and to take any calls, or texts outside of the building. All staff must be vigilant and remind any parents/visitors who forget
- We ask all parents/carers to sign an agreement about taking and publishing photographs, and videos of their children, and this list is checked whenever an activity is being photographed or filmed
- For their own protection staff or other visitors to school never use a personal device (mobile phone, digital camera or digital video recorder) to take photographs of pupils
- School mobile phones or similar devices with communication facilities used for curriculum activities are set up appropriately for the activity. Pupils are taught to use them responsibly
- Where required for safety reasons staff will contact their School and the school will contact parents. Staff will not use personal mobile phones in any situation where their mobile phone number or other personal details may be revealed to a pupil or parent
- Unauthorised or secret use of a mobile phone or other electronic device, to record voices, pictures or video is forbidden. Unauthorised publishing of such materials on a website which causes distress to the person(s) concerned will be considered a breach of school discipline, whether intentional or unintentional. The person responsible for the material will be expected to remove it immediately upon request and appropriate procedures followed.

Use of Other Technologies

- Each School will keep abreast of new technologies and consider both the benefits of learning and teaching, and also the risks from an eSafety point of view

- We will regularly review the eSafety policy to reflect any new technology that we use, or to reflect the use of new technology by pupils

- Staff or pupils using technology not specifically mentioned in this policy will be expected to behave with similar standards to behavior to those outlined in this document.

Links to Other School Policies/School Documents

- The Federation's eSafety policy will operate in conjunction with other policies including those for Child Protection and Safeguarding, Behaviour, Data Protection, Acceptable Use Policy for Staff and Senior Students, ICT and the Whistle Blowing Policy.

Appendix 1

ACCEPTABLE INTERNET AND EMAIL USE AGREEMENT FOR STAFF AND SENIOR STUDENTS

The computer system is owned by the School and is made available to staff and students to further their education and to enhance their professional activities including teaching, research, administration and management. This policy has been drawn up to protect the students, the staff and the School.

The School reserves the right to examine or delete any files that may be held on the computer system or to monitor any Internet sites visited.

- Access must only be made via the authorised account and password, which must not be made available to any other person

- All internet use should be appropriate to staffs' professional activity or student's education

- Activity that threatens the integrity of the School ICT system, or that attacks or corrupts other systems, is forbidden

- Sites and materials accessed must be appropriate for use in schools. Users will recognise materials that are inappropriate and should expect to have their access removed

- Users are responsible for email they send and for contacts made that may result in email being received

- The same professional levels of language and content should be applied as for letters or other media, particular as email is often forwarded

- Posting anonymous messages and forwarding chain letters is forbidden

- Copyright of materials and intellectual property rights must be respected

- Use for personal financial gain, gambling, political purposes or advertising is forbidden.

Staff and students requesting internet access must sign a copy of this and return it to the Senior Administration Office in the School for approval before access will be granted.

I confirm that I have received and read a copy of the School's Internet and Email Policy and agree to abide by it. I understand my accesses will be monitored.

Full Name: ..... Job Title: .....

Signed: ..... Date: .....

Access Granted: ..... Date: .....