ASHMORE PARK

AND

PHOENIX NURSERY SCHOOLS FEDERATION

DIGITAL SAFEGUARDING POLICY

Senior Leadership Team/Compliance Governor(s) Review Date	20.11.2023
Governing Board Approved/Adopted	*Chair's Action* *20.11.2023* Approved 07.03.2024
Signed on behalf of the Governing Board/Committee	
Policy to be Reviewed Date	30.11.2024

The Federation's Vision

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

This policy considers the use of both fixed and mobile devices with an appropriate internet connection e.g. iPods, 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 whilst in school, at home and within their local environment.

Equality and Inclusion

The use of technology is 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 in which everyone leads their life in the 21st Century. Technological advances are ever changing and when compared to even five years ago, the technology available outside school is rapidly increasing. In line with the Gilbert review document ***2020 Vision***, schools need to be increasingly aware of, and 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 use of online technological resources grow, so does the awareness of risks and potential dangers that arise from 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 approaches taken to achieve this.

Management of Digital Safeguarding

The Federation will ensure staff have 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
- Create and maintain eSafety policies and procedures
- Develop an understanding of current eSafety issues, guidance, and appropriate legislation
- 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 Together Board and other relevant agencies as appropriate
- Ensure that staff and children 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

- Always maintain a professional level of conduct in their personal use of technology

- 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 the incident to the Headteacher

- Respect the feelings, rights, values, and intellectual property of others in their use of technology, whilst in school 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

Staff who do not follow the 'Acceptable Use Policy for Staff and Senior Students' will be subject to the Federation's normal behavior and/or disciplinary procedures.

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

(Please see the Federation's Whistle Blowing Policy)

Incidents which pose a risk to the security of either school network, or create an information security risk, will be referred to the Federation's external specialist IT service provider, eServices, for technical support. Appropriate advice shall be sought, and action will be taken to minimise the risk and prevent further instances occurring, including reviewing all policies and procedures. If the action breaches the Federation's policy, appropriate sanctions will be applied. The Federation will determine if parents/carers need to be informed, if there is a risk that their children's data has been compromised.

The Federation reserves the right to monitor equipment on their premises and to conduct a search on any technological 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 'Child Protection' concerns, up to date guidance will be taken directly from the Local Authority's, Wolverhampton Safeguarding Together Board, which can be located at https://www.wolverhamptonsafeguarding.org.uk/, all recommendations will be implemented and directions observed.

Risks and Acceptable Behaviors

General use of the internet - Children will only access the internet when a supervising adult is nearby, however, 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 continued professional development of staff as an essential tool
- Enhance each School's management of information and business administration systems
- Enable electronic communication between staff, parents/carers
- Facilitate the exchange of Curriculum and administration data with the Local Authority.

All staff are aware that they are responsible for their behaviours when using the school's ICT equipment e.g. assigned laptop(s), the School's IT systems e.g. shared drive, or electronic device(s) e.g. assigned iPod(s), all of which are provided by the School. Staff understand that all activity is monitored and is subject to safety checks.

All staff will be required to always abide by the relevant 'Acceptable Use Policy for Staff and Senior Students', which includes working under supervision or independently.

Password/Personal Details

Staff should abide by the rules outlined in the 'Acceptable Use Policy for Staff and Senior Students' (Appendix 1), in which staff are advised that it is good practice to change passwords periodically to enhance 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 practices and procedures to ensure that both schools observe the necessary statutory recommendations.

Each School is a registered Data Controller and complies with the data protection principles outlined in the Data Protection Act 2018, https://www.gov.uk/data-protection, which is the United Kingdom's implementation of the General Data Protection Regulation (GDPR), now UK GDPR.

Procedures are in place and where necessary, training is provided, to ensure the security of all data, which includes the following:

- All computers and laptops, holding sensitive information have password settings in place, they have password protected screen savers and screens are locked by the user when they are left unattended
- Individual staff are assigned the appropriate level of access to their school's information management systems, which hold pupil data. Under no circumstances are passwords shared
- Staff are aware of their obligation to keep sensitive data secure when working on computers outside school
- We follow the City of Wolverhampton Council's procedures for transmitting data securely
- Remote access to shared drives etc. is subject to authorisation by the Headteacher and is applied to individual personnel to meet the needs of each School/Federation
- The Federation has secure backup and recovery procedures in place for both School's data
- In the event that sensitive data has to be shared with external parties/professionals e.g. Governors or the Federation's School Improvement Partner (SIP), the school will label the documentation appropriately, all parties will be notified that the information is Confidential, and all hard copies will be destroyed.

E-mail

Email is regarded as an essential means of communication. Communication by email between staff, parents/carers and the wider school community will be sent via the applicable School's secure email account or the member of staff's assigned 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's address, e-mail, and telephone number
- Identities of children are always protected. Photographs of identifiable individual children are not published on the website unless the respective School obtains written permission

from parents/carers to use their child's photograph. Group photographs do not have a name list attached

- Staff are encouraged to adopt safe and responsible behaviors when using blogs, social networking sites and other online sites for personal use

- Materials published by children, Governors and/or staff in a social context, which are considered to bring their School into disrepute, are considered harmful to the school, or are deemed to be harassing a member of the school community will be considered a breach of the Federation's policies and procedures, and may be subject to disciplinary proceedings.

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 are located securely with only appropriate staff permitted access. Servers, workstations and other hardware and software are kept updated as appropriate. A firewall is maintained, 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

- All administrator or master passwords for school ICT systems are kept secure, however, are 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, and all users have to be granted access by a member of the eServices technical support team

- We do not allow anyone except members of the eServices technical support team to download and install software onto the network.

Filtering and Monitoring

- In line with the Department for Education's filtering and monitoring standards, the Federation has:

    - Identified and assigned roles and responsibilities to manage filtering and monitoring of systems. Web filtering of internet content is currently provided by the City of Wolverhampton Council, which ensures that all reasonable precautions are taken to prevent access to inappropriate material. The Headteacher and Governors are responsible for ensuring these standards are met by reviewing the effectiveness of the IT provision, overseeing reports, documenting decisions around the IT provision and ensuring staff understand their role in following policies and procedures. The Federation will work with the City of Wolverhampton Council to ensure that these needs are met, any risks are identified, and reviews are carried out

    - The filtering and monitoring provision will be reviewed annually or when a new risk has been identified to evaluate any changing needs and risks. The Headteacher, Governors and the City of Wolverhampton Council who are the current provider will carry out the review

- Harmful and inappropriate content will be blocked without unreasonably impacting teaching
  - It is not, however, possible to guarantee that access to unsuitable material will never occur. Staff are encouraged to check websites that they wish to use prior to their use with the children
    - If staff require access to a 'blocked' site they must contact the DSL for approval, the DSL will assess the site's suitability and contact eServices to allow staff access to the site, as and when appropriate.
  - All users are informed about the action they should take if inappropriate material is accessed or discovered on a computer
- There will be effective monitoring strategies that meet the safeguarding needs of each school
  - Weekly monitoring will be undertaken by the Headteacher and recorded on the 'Federation Filtering and Monitoring Tracker', (See Appendix 2)
- User activity will be monitored on school devices. Any incidents will be acted on and the outcome recorded
- Staff will supervise the use of devices and report any safeguarding concerns
- The Headteacher will decide 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. Temporary internet access can be granted by a member of the eServices technical support team for all visitors, as and when required
- All users are provided with a log in appropriate to their 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, and procedures are in place to ensure login and password information remains secure and is protected.

Mobile Phones/Technology

- We recognise that many aspects of the Curriculum can be enhanced using 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 prior permission of the parents/carers of the participants, and all images and videos are of appropriate activities. Full names of participants are not used either within the resource itself, within the file name or in accompanying text

- All parents/carers/visitors are asked not to use mobile phones when in either school, or are requested to take all calls, or to respond to texts outside the building. All staff must remain vigilant at all times and remind any parents/carers/visitors of the Federation's safeguarding procedures

- 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 by the applicable child's Educator

- For their own protection, staff or visitors to school never use a personal device e.g. mobile phone, digital camera, or digital video recorder to take photographs of children

- School mobile phones or similar devices with communication facilities used for Curriculum activities are set up appropriately for the activity. Children are taught how to use them responsibly

- In the event of an accident/emergency, staff will contact their applicable School and the school will contact parents/carers accordingly. Staff will not use personal mobile phones in any situation where their mobile phone number or other personal details may be revealed to a child or parent/carer

- 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 the Federation's policies and procedures, whether intentional or unintentional, and may result in disciplinary action. 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 will consider both the benefits to learning and teaching, whilst also considering any eSafety risks

- The Senior Leadership Team will regularly review the Digital Safeguarding Policy to ensure it reflects any new technology introduced across the Federation, or to reflect the use of new technology by its children

- Staff and/or children using technology, not specifically mentioned in this policy, will be expected to behave with similar standards as outlined in this document.

Links to Other School Policies/School Documents

- The Federation's Digital Safeguarding Policy will operate in conjunction with, however, is not exhausted to the Safeguarding and Child Protection Policy, the Behaviour Policy, the Data Protection Policy, the Acceptable Internet and Email Use Agreement for Staff and Senior Students, Employee Code of Conduct & Expected Standards Policy, Information Governance Policy, the Social Media Policy and the Whistle Blowing Policy.

Appendix 1

ACCEPTABLE INTERNET AND EMAIL USE AGREEMENT FOR STAFF AND SENIOR STUDENTS

All computer system(s) are owned by the applicable School and are made available to staff and students to further their education and/or to enhance their continued professional development through teaching, conducting research, completing administration duties and applying management strategies. This policy has been created to protect students, staff, both schools' and the Federation.

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

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

- All internet use should be appropriate to staffs' continued professional development or the student's education

- Activity that threatens the integrity of the School's ICT system(s), or that attacks or may corrupt other school system(s) 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 the emails that they send and for all professional contacts made, they must therefore; ensure all email usage is appropriate and applicable to the school. Users should note that emails can be forwarded to multiple recipients

- The same level of professional language and content should be applied to emails, as is applied to letters and other forms of business communication

- Posting anonymous messages and forwarding chain letters is forbidden

- Copyright of materials and intellectual property rights must be respected

- Use of school property or school platforms for personal financial gain, gambling, political purposes, or advertising is strictly forbidden and may result in disciplinary action.

Staff and students requesting internet access must sign a copy of the agreement and return it to the Senior Administrator, in the applicable school's office for approval, prior to access being authorised and granted.

I confirm that I have received and read a copy of the Federation's Social Media Policy and agree to abide by it. I understand my access/use will be monitored and could be removed at any time.

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

Signature: .... Date: ....

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

Ashmore Park
Nursery School

FEDERATION FILTERING AND MONITORING TRACKER

Phoenix
NURSERY SCHOOL

Appendix 2

DATE	SCHOOL MONITORED	ISSUES IDENTIFIED/INVESTIGATED	ACTION TAKEN	SIGNATURE