ASHMORE PARK

AND

PHOENIX NURSERY SCHOOLS FEDERATION

DIGITAL SAFEGUARDING POLICY

Senior Leadership Team Review Date	17.10.2025
Governing Board Approved/Adopted	21.10.2025
Signed on behalf of the Governing Board/Committee	C.A. Lingard-Jones
Policy to be Reviewed Date	30.11.2026

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 forms part of the Federation's 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 structures are 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 Internet and Email User Agreement for Staff and Governors' (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 can carry out their roles effectively in regard to eSafety
- Receive and regularly review Federation eSafety filtering and monitoring Senso alerts; investigate and record all issues identified and any action(s) taken; ensure that the correct procedures are followed should an eSafety incident occur in either school, and conduct analysis of all incidents to identify if further action is required or change to policy or procedure is necessary, to safeguard our school communities
- Promote the 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 Federation's 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 Internet and Email User Agreement for Staff and Governors'
- Liaise with the Local Authority (LA), the Wolverhampton Safeguarding Together board and other relevant agencies as and when appropriate
- Ensure that staff know the procedure to follow should they encounter any material or communication that makes them, or their children, feel uncomfortable.

Responsibilities of the Governing Board

That the Safeguarding Link Governor liaises with the Headteacher; monitors practices and procedures, 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 'Acceptable Internet and Email User Agreement for Staff and Governors'
- 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, to the Headteacher immediately for investigation, and where necessary escalation to the Federation's external specialist IT service provider, eServices, for remedial action
- Respect the feelings, rights, values, and intellectual property of others in their use of technology, whilst in either school or at home.

Responsibilities of the Parent/Carer

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

Procedures

- Staff who do not follow the 'Acceptable Internet and Email User Agreement for Staff and Governors' will be subject to the Federation's 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 for further guidance.**

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, and if there has been 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

Routine use of the internet:

- Children will be supervised by their Educator when accessing the internet in school, in addition, there is a robust filtering system in place across the Federation to safeguard children when technology is in use.

We provide access to 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 and 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 their school's ICT equipment e.g., assigned laptop(s), their school's IT systems e.g., shared drive, or electronic device(s) e.g., assigned iPhone(s), all of which are provided by their applicable school. Staff understand that all activity is monitored and is subject to safety checks.

All staff are required to adhere to the 'Acceptable Internet and Email User Agreement for Staff and Governors', which includes when working under supervision or independently.

Password/Personal Details

All staff should abide by the guidance included in the 'Acceptable Internet and Email User Agreement for Staff and Governors' (Appendix 1). In addition, staff are advised to change their passwords periodically to enhance data security, to use alphanumeric passwords that include a special character, and to not use the same password for multiple sites etc.

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 alphanumeric passwords that include a special character 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 staff and pupil data. Under no circumstances are passwords shared
- Staff are aware of their obligation to keep sensitive data secure when working offsite e.g. at home on a school laptop
- 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 members of staff, to meet the needs of each School/Federation
- The Federation has secure backup and recovery procedures in place for both school's data
- If sensitive data has to be shared with external parties/professionals e.g. Governors or the Federation's 'School Improvement Advisor' (SIA), the applicable 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 between staff, parents/carers, external professionals and the wider school community. For security purposes all school email accounts are regularly monitored. All correspondence will be sent via the applicable school's secure account or

the staff member's assigned school email account.

All email communication should be related to school matters only to ensure that the good name of the Federation and its schools are maintained. Email messages should be clear and concise and have a professional tone, they should not contain slang terminology, excessive exclamation points, and should not contain humour as this could be misconstrued and/or deemed unprofessional/ inappropriate.

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 action.

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; 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 administration/master passwords for school ICT systems are kept secure; however, they are available to at least two members of staff e.g. Headteacher and School Business Manager/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 Headteacher for approval, the Headteacher 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 all school devices, all incidents will be investigated, the necessary action taken, as and when applicable, 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 requested by the Headteacher
- 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 remain secure and is protected.

Mobile Phones/Technology

- We recognise that many aspects of the Curriculum can be enhanced using multimedia 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 by staff 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, which includes taking/answering a telephone call, or responding to a text until outside of the school building. All staff must always remain vigilant 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 everyone's protection, staff and visitors to school never use a personal device e.g. a smart watch, a mobile phone or a digital camera to take photographs of children.
- School iPhones, iPads or similar devices with communication facilities used for Curriculum activities are set up appropriately and children are taught how to use them responsibly
- In the event of an accident/emergency, staff will contact their applicable school, and the school representative will contact individual 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 undisclosed use of a mobile phone or other electronic devices, to record voices, pictures or video is strictly forbidden

- Unauthorised publishing of any digital material on a website, which causes distress to the person concerned will be considered a breach of the Federation's policies and procedures, whether intentional or unintentional. The person responsible for the material will be expected to remove it immediately upon request and they may be subject to disciplinary action.

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

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 User Agreement for Staff and Governors, Employee Code of Conduct & Expected Standards Policy, Information Governance Policy, the Social Media Policy and the Whistle Blowing Policy.

Appendix 1

ANNUAL RENEWAL
ACCEPTABLE INTERNET AND
EMAIL USER AGREEMENT FOR STAFF AND GOVERNORS

All services that can access the internet are owned by the Federation, are utilised in each school and are made available to staff to enhance their professional activities including teaching, research, administration and management. The Federation's 'Acceptable Internet and Email User Agreement' has been drawn up to protect all parties; Children, Students (on placement), Staff and Governors across the Federation.

The Headteacher reserves the right to examine or delete any files that may be held on any mobile device or to monitor any internet usage.

- 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 the users' professional activity;

- Activity that threatens the integrity of either school's ICT system, or that attacks or corrupts other systems, is forbidden;

- Sites and materials accessed must be appropriate to work conducted in or on behalf of the applicable School/Federation. Users who access materials that are inappropriate should expect to have their access removed and the appropriate disciplinary action taken;

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

- The same professional level of language and content should be applied to all forms of media, particularly emails as they are often forwarded, as would be applied to letters;

- Posting anonymous messages and forwarding chain letters is strictly forbidden;

- Copyright of materials and intellectual property rights must be respected;

- Use for personal social media platforms, financial gain, gambling, political purposes or advertising is forbidden;

- Downloading of any additional Apps by individual staff is strictly forbidden, which includes Artificial Intelligence (AI) Apps and all associated software.

All Staff and Governors across the Federation who have been allocated a school email account or granted access to Microsoft Office; Microsoft Teams; You Tube the internet etc. via any mobile device must sign a copy of this agreement annually to confirm that they have read the above information pertaining to the Federation's 'Acceptable Internet and Email User Agreement' and agree to abide by it.

All users understand that their access and permissions will be monitored and removed if abused, and the appropriate disciplinary action will be taken.

Annual Declaration

I confirm that I have read the Federation's 'Employee Code of Conduct and Expected Standards Policy and the 'Social Media Policy' and agree to abide by them.

I understand that my ICT access and usage will be monitored and could be removed at any time, and that if found in breach of any Federation policy the appropriate disciplinary action will be taken in line with the guidance stipulated in the Federation's 'Disciplinary Policy and Procedure' document.

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

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

For New Users:

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

Appendix 2

FEDERATION FILTERING AND MONITORING TRACKER

DATE	SCHOOL MONITORED	ISSUES IDENTIFIED/INVESTIGATED	ACTION TAKEN	SIGNATURE