Stow Heath
Primary School

Digital Safeguarding Policy

Stow Heath Primary School, Hill Road, Portobello, Willenhall, WV13 3TT
Telephone: 01902 558820   Fax: 01902 558821
Email: stowheathprimaryschool@wolverhampton.gov.uk

Shine like a Star

School Vision

Why do learners need access to the latest technology for their education and wellbeing?

Technology is now considered to be an essential part of modern life. In addition, the school has a duty to provide pupils with quality technology as part of their learning. This digital safeguarding policy considers the use of both the fixed and mobile devices with an appropriate internet connection, 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 purpose of technology use in school is to help deliver the whole school aims; To offer a curriculum that is enhanced by integrating ICT across all subject areas, promoting enjoyment, a personal sense of fulfillment, achievement and the life skills that will help our children thrive in the 21st Century..
At Stow Heath Primary School we aim to provide the best possible educational opportunities for all children to achieve their full potential and become e-confident learners by providing a creative curriculum designed to meet the needs of all our children, with equal access for all.
Through our teaching we aim to:

- Enable children to become imaginative, innovative, creative thinkers
- Develop in each child a sense of self-esteem, responsibility and confidence
- Help each child to develop the ability to share and co-operate with others
- Encourage children to respect ideas, attitudes, values and feelings of others
- Encourage a sense of community and good citizenship
- Enable personal development and promote children's spiritual, moral, social and cultural development
- Equip the children with essential learning skills of communication, application, problem solving and evaluation
- Promote children's physical, emotional health and a healthy lifestyle
- Make learning enjoyable and fun
- Encourage children to be safe when using digital technology

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 pupils. Internet access is an entitlement for all. However, responsible and safe use must be at its core, this is outlined in the AUP documents.
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. 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 learners need to be safe working with technology?
As the uses of online technological resources grow, so has the awareness of risks and potential dangers which arise for their use. This school 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 –

- What is the role and responsibility of the Head teacher?

  The Headteacher will ensure that the digital safeguarding policy is implemented and compliance with the policy monitored, and that the appropriate roles (see this section) and responsibilities of the school's digital safeguarding structure is in place. Ensure regular reports of the monitoring outcomes on digital safeguarding are reported to the governing body.
- What is the role and responsibility of the nominated digital safeguarding coordinator?

  There is an identified e-safety coordinator who is responsible for e-safety developments in school and sharing of practice with staff and the wider community. This person needs to be in receipt of current training on the latest guidance and procedures. They are the main contact for the Local Authority e-Safety networks. All digital safeguarding incidents within the school need to be reported to this person. They need to keep the log of incidents and with the Head teacher make decisions about how to deal with reported incidents
- What is the role and responsibility of the E-Safety governor?

  There is an identified e-safety governor who monitors and liaises with the e-safety coordinator. They will report to full governing board as appropriate.
- What is the role and responsibility of the subject co-ordinators?

  All staff with subject and management roles have a duty to incorporate e-safety principles in their area of responsibility, deputising for any of the above roles where appropriate.
- What is the role and responsibility of the class teacher?

All staff understand the need for care and caution when using technology both for academic and social purposes and apply it to teaching and learning situations. They need to work to agreed guidelines (AUP and Social networking guidelines – see appendix) They have a "front line" monitoring and reporting role for incidents.

- What is the role and responsibility of the support staff?

As for teaching staff, however, given the nature of their role, learners may find it easier to disclose incidents to them. Support staff should be clear of the reporting procedures

- What is the role and responsibility of the Leadership Team representatives?

As a responsible member of their class the Leadership Team need to have e safety on their agenda as an item. These representatives could help to monitor at a learner level the appropriate use of technology within the school.

What are the procedures?

- Internal reporting procedures – If staff or pupils discover unsuitable sites or encounter unsuitable practises the safeguarding or ICT co-ordinator will need to be informed. These would be logged and when required reported to the Governors.
- External reporting procedures – Once inappropriate sites or behaviours have been disclosed to the safeguarding or ICT co-ordinator, it will then need to be assessed as to the seriousness of the incident. If unsure the co-ordinator would then contact the e-services team for advice or in extreme cases the police would need to be informed.
- Incident log – A log is kept by the Head of any incidents regarding digital safeguarding issues. It is a requirement that all incidents are reported to the Governors on a regular basis.
- Signing agreements

  Staff – Staff are required to sign and adhere to a school laptop agreement and an acceptable use agreement.

  Parents – Parents are required to sign an agreement that allows their child to use the ICT equipment at school, have access to the internet and allows school to take and use digital photos and video for school use only.

  Pupils – Pupils are required to sign and adhere to the pupil acceptable use agreement

  Governors – Governors are required to sign and adhere to the governors acceptable use agreement
- Staff training

  The ICT-co-ordinator will attend various courses that will benefit the school. The ICT co-ordinator will be responsible for identifying the ICT needs of the staff and delivering staff development accordingly. Staff will also have entitlement to access other training delivered by the e-services team and other outside agencies.
- Monitoring

  The ICT co-ordinator with the support of the Head will be responsible for monitoring the implementation of all ICT and e-safety documents and policies. They will also be responsible for monitoring the use of the Internet and e-mail.

What are the risks and acceptable behaviours?

- General use of the internet

  Whilst staff are at school or using a school laptop they should adhere to the guidelines set out in the staff laptop agreement and staff AUP. Staff must also be aware that online activities and behaviours should reflect the professional nature of their work and not compromise the reputation of the school or local authority. The use of the internet by pupils in school is monitored and filtered by the LA technical solution. (See appendix 3) Opportunities for T& L related to e-safety are built into the curriculum and e-safety is taught discreetly each term and when the need arises. The Pupil AUP is shared and signed with pupils to ensure they understand how to stay safe online.
- Passwords/personal details

  Staff - All staff are assigned usernames and passwords in order to access the school server. All staff are required to register on Engage and will receive a username and a password that can be changed to suit. They will also be assigned a school e-mail address, it is advised that staff use this email address for work purposes only as personal emails cannot be accessed on the school internet system and school emails are monitored externally by LPPlus.

  Pupils – All pupils are assigned user names and passwords in order to access the Learning Platform.

  Governors – All Governors have the right to resister for an account on the Engage website. This will allow them access to the schools Learning Platform.

  Parents - Parents are assigned a generic password that will allow them to access the school Learning Platform.

  Passwords and personal details should not be shared with anyone else. It is a breach of the data protection act to use someone else's password. This behaviour will result in the Head taking further action. Staff are required to follow the guidance set out by the authorities HR department regarding online social networking sites. (See appendix 1) It will be deemed a disciplinary offence should these guidelines not be adhered to.
- Data Security – Staff should refrain from storing pupil data, including pictures, videos and personal details on laptops or memory sticks. The learning Platform should be used where possible to have access to such data.
- E-mail – Staff must use their school email address for work related communications. Where possible the learning platform should be used to share potentially sensitive pupil data. It is suggested that staff refrain from emailing any sensitive pupil data or personal details.
- Learning Platform – Guidance on the use of the LP is covered by the schools AUP for staff and pupils. The LP provides a safe platform for pupils and staff to interact and any provides a secure storage facility for sensitive pupil data. Staff, pupils and parents must understand that online behaviours must be appropriate and that any inappropriate behaviours will be reported and dealt with in line with school policy.
- Appropriate use of hardware – Staff use of hardware is covered by the schools laptop agreement and staff AUP. Children must sign the schools AUP which covers the use of hardware including laptops, cameras (Still and video), bee bot, Roamer. (see pupil AUP appendix 3)
- Photographs, video and sound recording – Photographs that include pupils will be carefully selected so that individual pupils cannot be identified or their image misused.. pupils full names will not be used anywhere on the school website or other on-line space,

particularly in association with photographs. written permission
from parents or carers will be obtained before photographs of pupils are published on the school web site. Parents are required to sign a permission slip allowing the school to use any suitable photos or work from their child.

- Copyright – Staff will not knowingly use copyrighted materials e.g. Use unauthorised picture from the internet for teaching resources. Where possible staff will always use copyright free resources including music and sound files. (All resources from Espresso can be used by Wolverhampton teachers.)
- Social networking/cyber bullying - Staff are required to follow the guidance set out by the authorities HR department regarding online social networking sites.   (See appendix 1) It will be deemed a disciplinary offence should these guidelines not be adhered to. Should a child be involved in any cyber bullying issues they should be dealt with according to the internal and external reporting procedures and appropriate action taken?
- Mobile phones – The use of mobile phones by staff and pupils must be used in line with the schools AUP.

What physical and technical security is available?

Firewall provision, Filtering provision, Antivirus software – See
E-Safety Infrastructure Overview, Wolverhampton Children & Young People appendix 2

The school has a main server system which controls the following throughout the school:

- A high filter system, therefore preventing unsuitable sites to be accessed by children and staff.
- Only licensed software is used within the school. Copies of all licenses are kept securely in the school office.
- Virus protection will be updated regularly.
- School ICT systems security will be reviewed regularly.
- Any personal data sent over the internet will only be sent securely from and to authorised sites and is stored on password protected machines
- Virus protection is installed and updated regularly.
- Personal software is not allowed.
- The e-mail system is used under a secure filter system and all staff have a school e-mail address and are strongly advised to use it for school use.

What is the impact of the Digital Safeguarding Policy?

- Awareness of Learner access (Risk) via the ICT@home survey
- Usage monitoring reports from the learning platform
- Monthly report of incident log
- Internal monitoring of internet /network activity
- Minutes of school council

What are the links to other school policies and school documents?

Reference to digital safeguarding are made in the following documents -

- Staff handbook
- Reference in SEF
- Reference in SIP
- Curriculum plans
- Reference in other school policies
- School handbook
- Job descriptions
- School prospectus

Resources

Resources needed to train and support Workforce

- E safety briefings by LA
- US online digital resource
- e-safety site
- Staff meetings led by LA and ICT Co-ordinator
- CEOP web site

Resources needed to train and support Learners

- US online digital resource
- CEOP web site
- ICT scheme of work

Resources needed to train and support Families and Governors

- Governor training led by LA and ICT Co-ordinator
- Resources made available on the school learning platform
- US online
- Governors site on Engage.