E-safety Policy

E-Safety encompasses internet technologies and electronic communications such as mobile phones and wireless technology. Holding an E-Safety policy highlights the need to educate professionals, parents/carers and children about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

E-Safety depends on effective practice on a number of levels:

- Responsible ICT use by all staff, children and Parents/Carers, made explicit through policies.
- Sound implementation of E-Safety policy in both administration and curriculum, including secure network design and use.
- Safe and secure broadband, including the effective management of content filtering.

Internet use

The purposes of Internet use in the Nursery setting are to raise educational standards, to promote achievement, to support the professional work of staff and to enhance management information and administration systems.

Internet use is a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for staff and parent/carers who show a responsible and mature approach to its use. Our Nursery has a duty to provide quality Internet access.

Benefits of using the Internet in education include:

- Access to learning wherever and whenever convenient
- Access to world-wide educational resources
- Educational and cultural exchanges world-wide
- Access to experts in many fields for parent/carers and staff
- Professional development for staff through access to national developments, educational materials and effective curriculum practice
- Collaboration across support services and professional associations
- Improved access to technical support including remote management of networks and automatic system updates
- Exchange of curriculum and administration data with the Local Authority and other bodies

It is acknowledged that, despite the benefits offered by the Internet, unlimited Internet use can have a detrimental effect of the wellbeing of the children Staff and parents/carers should therefore be taught what Internet use is acceptable and what is

not and given clear objectives for Internet use. Internet access should be planned to enrich and extend learning activities.

All ICT resources at the school have filtering systems which prevent access to unsuitable sites.

All staff must read and sign the 'Code of conduct for school employees' before using any ICT resource at the Nursery setting. All staff will be given the E-Safety Policy and its importance explained during Induction. Staff and parents/carers should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential. Staff and partners that manage filtering systems or monitor ICT use will be supervised by management and have clear procedures for reporting issues. If staff and parents/carers discover unsuitable sites, the URL (address), time and content must be reported to the Local Authority helpdesk via the Head teacher.

It is the Head teacher's responsibility to ensure that the use of Internet derived materials by staff and parents/carers complies with copyright law. Staff and parents/carers should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy. The Nursery School will work to ensure filtering systems are as effective as possible.

Email

Staff and parents/carers must immediately tell the Head teacher if they receive offensive e-mail. E-mail sent to external organisations from staff should be written carefully and agreed by a member of SLT before sending. Reference requests must be referred to the Head teacher and should not be sent from anyone acting in their capacity as an employee of the school without reference to the Head teacher first. , in the same way as a letter written on headed paper. The forwarding of chain letters is not permitted.

Mobile Phones

No adults are to use mobile phones in classrooms when children are present. This particularly includes camera (smart) phones and video.

If a staff member needs to take an emergency call, permission must be agreed by a member of the Senior Leadership team.

This rule will be explained to all Parents/Carers at the first contact and repeated at the first session of any course or group in which they are participating.
- If any adult needs to use a phone then they must leave the room and inform a practitioner that they are leaving the room.
- Parents/Carers using mobile phones at any time whilst in a shared learning environment, including Forest School sessions, and on bus journeys, will be asked by staff to turn them off.

- Parents/Carers using mobile phones during settling-in visits into the Nursery setting will be asked to turn them off. At other times, they will be asked to use them in the corridor or foyer.
- Visitors to the Nursery setting, including students and professionals, will be asked to leave their phone in the reception office where they will be kept in the secure drawer.
- All photographic images remain the property of the Nursery and permission to use them will be sought from Parents/Carers; i.e. separate written consents are sought for use within the Nursery, for publication on the Nursery website and for use in other publicity.

Social Networking

St Werburgh's Park Nursery School will block/filter access to social networking sites and newsgroups unless a specific use is approved. Staff will be advised never to give out personal details of any kind which may identify the Nursery School, or to 'friend' parents/carers. Staff and parents/carers should be advised not to place Nursery photos on any social network space.

Staff must not post information about the school and/or other employees children or parents on any social media without the permission of the Head teacher. If permission is given the Head teacher will ensure the permission of any parent is also received before posting any information relating to a parent and/or child.

School Equipment

School equipment and systems, including portable equipment (phone, email and computers) are available only for school-related activities. They must not be used for any activity that is illegal, unacceptable or inappropriate to the good conduct of school's business or for the fulfilment of another job or for personal use unless authorised by the Head teacher (for the Head teacher authorisation is from the Chair of Governors).

Examples of misuse include;

- Creating, sending or forwarding any message that could constitute bullying or harassment (on the grounds of a 'protected characteristic') or whose content or intent would reasonably be considered inappropriate or unacceptable;

- Participating in forwarding chain letters, pictures or graphics etc.

- Accessing pornography;

- Committing or implying commitment to any contractual arrangements;
- accessing, publication or circulation of illegal, offensive, unacceptable, inappropriate or non-work related material;

- Any illegal activities;

- Gambling or gaming;

- Accessing any non-work related or otherwise inappropriate or unacceptable material.

- Employees receiving inappropriate communication or material or who are unsure about whether something they propose to do might breach this policy should seek advice from their Head teacher.

- Employees are responsible for taking reasonable steps to ensure the safety and security of any school equipment provided to them and must return it to the school when they leave employment, or on the request of the Head teacher.

Managing emerging technologies
Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use is allowed.

St Werburgh's Park Nursery School website
The contact details on the website will be the address, e-mail and telephone number. Personal information will not be published.

Publishing children's images and work
Photographs that include children will be selected carefully and will be appropriate for the context. Parents/carers and children's full names will not be used anywhere on the Website, particularly in association with photographs. Written permission from parents/carers will be obtained at the beginning of the school year for photographs of children that may be published on the school website any time after the permission is given. Work can only be published with the permission of parents/carers.

Information system security
School ICT systems capacity and security will be reviewed regularly. Virus protection is installed and updated regularly. Security strategies will be discussed with BCC/ contracted partners by the Head teacher as necessary.

Passwords must not be shared and access to computer systems must be kept confidential.

Protecting personal data
Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and General Data Protection Regulations 2018.

Assessing risks
The Nursery School will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a Nursery School computer. We cannot accept liability for the material accessed, or any

consequences of Internet access. We will audit ICT use to establish if the E-Safety policy is adequate and that the implementation of the E-Safety policy is appropriate.

Handling e-Safety Complaints

Complaints of Internet misuse will be dealt with by the Head teacher. Complaints about abuse must be dealt with in accordance with the relevant procedure(s) and this may include Child Protection procedures. Parents/Carers will be informed of the complaints procedure.

Parents/carers info

Parent/carers attention will be drawn to the E-Safety Policy in newsletters and on the website.

Monitoring

The Head teacher will be responsible for monitoring the use of computer systems, including access to websites, the interception of e-mail and the deletion of inappropriate materials where it is believed unauthorised use of the computer system may be taking place, or if the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Written: March 2021
Next Review date: March 2024