Watergate School

E-safety Policy

This policy was agreed by the Headteacher on: (and supersedes all previous policies relating to this area)	
Signed by: (Headteacher)	
Implemented: February 2018	
Interim Review and update : Spring 2019 Carolyn Vagg	
Review date: February 2022	
Author: Jesus Jimenez Gazquez – Lead professional for ICT/Middle Leader	

Context

Internet safety has been a compulsory part of the curriculum since 2014, as well as measures in place to prevent cyber-bullying.

Watergate School is a primary school that caters for the needs of children with severe and profound learning difficulties, most of whom have additional physical, sensory, and behavioural challenges. Some of our pupils have complex medical needs and most have significant social and communication difficulties.

E-safety encompasses technology and covers issues relating to children and young people as well as adults and their safe use of the Internet, mobile phones and other electronic communications, both in and out of school. It includes education for all members of the school community about risks and responsibilities and is part of the 'duty of care' that applies to everyone working with children. Most children at Watergate School are unable to access technology independently but those who can, will be closely supervised.

Aims

- Safe and responsible use of technology by all children and staff;
- Implementation of e-safety policy and practice, ensuring all users are aware and fully comply with all relevant legislation;
- Safe and secure infrastructure (use of internet and filtering systems).

Teaching and Learning

We believe that, in the 21st Century, children, young people and adults interact with an increasing number of technologies on a daily basis. The learning opportunities that arise from this interaction are infinite but also potentially dangerous unless their safe use, both in school and outside school, are addressed as a matter of priority and are updated regularly.

The school has a duty to provide relevant and curriculum experiences enhancing the internet access to children as appropriate to their learning needs. Internet use is part of the statutory curriculum and is a necessary tool for learning.

Most of the issues concerning online safety are linked to the behaviour of users. It is therefore considered essential that our online policies, procedures and practices are developed with the aim of modifying those behaviours and promoting acceptable use.

We recognise that an unsecured online environment is a public place and that Information shared online on unsecured sites will be held in the public domain. We know there are significant implications around data security, how personal data is to be hold and processed and who will have access to it. As with any form of safeguarding, the potential risks to children and young people are acknowledged.

At Watergate, internet access will be provided to children with as much support as is necessary to enable access. This takes the form of browsing websites with appropriate filtering in place and adult guidance or using any content (e.g. pictures, videos) in any format to support teaching resources (e.g. PP Presentations, printed format, switch accessible programmes).

Where relevant, we will teach pupils about acceptable internet use and what is not and will be given clear lesson objectives for internet use.

We will ensure that the use of internet-derived materials by staff and children, complies with the copyright law.

At Watergate School, any children who are using e-mail as part of their curriculum for Computing and ICT, will be given a school approved e-mail address. Their use will be carefully monitored and e-mails will be shared within lessons. This ensures that any potentially offensive material will be screened and removed and children’s personal details will not be disclosed.

School website

- No personal information about staff or children will be published on the school website;
- Any photographs/video/information will be carefully managed and permission sought ensuring no personal information is disclosed;
- Children’s full names will not be used anywhere on the website, particularly in association with photographs;
- Written permission from parents or carers will be obtained before any material is published on the school website;
- The contact details on the website will be the school address, email and telephone number. Staff or pupil’s personal information will not be published.

Managing e-mails

- Staff will only use official school-provided email accounts to communicate with pupils and parents/carers/other professionals, as approved by the e-Safety leader;
- Staff will contact the network manager to recover an account/ password if forgotten.

Filtering

- Access to social networking sites will be blocked but access for specific supervised activities may be allowed (e.g. Skype, Facetime, Messaging, e-mail);
- The school will have a clear procedure for reporting breaches of filtering;
- If staff or children discover unsuitable sites, it will be reported to the e-Safety leader.

Video-Conferencing

- Any form of video-conferencing will be carefully planned and monitored, and will use the educational broadband network rather than the Internet.
- Children will only access this form of communication under staff permission and supervision;
- Parents and carers consent should be obtained prior to children taking part in video-conferences.

Managing Information Systems

- The security of the school information systems and users will be reviewed regularly;
- Virus protection will be updated regularly;
- Files held on the school's network will be regularly checked;
- The network manager will review system capacity regularly;
- The use of user logins and passwords to access the school network will be enforced.

Managing Emerging Technologies

- Emerging and new technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Protecting Personal Data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018

Managing Internet Access

- All staff must read and sign the ‘Acceptable Use Policy Agreement’ before using any form of technology;
- The school will keep a up-to-date record of all staff and children who are granted internet access at all times.

Assessing Risks

- The school will take all reasonable precautions to ensure the right balance between controlling access to the internet and technology, setting rules and boundaries and educating pupils and staff about responsible use. However, we recognise that children and staff cannot be completely protected from exposure to risks both on and offline. No child will be allowed unsupervised access to the Internet;
- The school will audit provision to ensure that the e-Safety Policy is adequately implemented and effective.

Handling e-safety complaints

- All members of the school community will be made aware of the importance of good e-Safety practice in the classroom in order to educate and protect the children in their care. Members of staff also need to be informed about how to manage their own professional reputation online and demonstrate appropriate online behaviours compatible with their role;
- Breaches of an e-Safety policy can lead to civil, disciplinary and criminal action being taken against staff, pupils and members of the wider school community. It is crucial that, at Watergate, we are aware of the offline consequences that online actions can have;
- Any complaints will be dealt with and recorded by the Child Protection Officer at school;
- All e-Safety complaints and incidents will be recorded by the ICT Lead, including any actions taken and the Head teacher informed

Internet Use across the Community

- The school will liaise with local organisations to establish a common approach to e-Safety;
- The school will be sensitive to Internet-related issues experienced by pupils out of school;

- The school will provide appropriate levels of supervision for students, who use the internet and technology whilst on the school site;
- The school will provide an AUP for any guest who needs to access the school computer system or internet on site.

Staff Use of Personal Devices

- Staff are not permitted to use their own personal phones or devices for contacting pupils, young people and their families within or outside of the setting in a professional capacity;
- Mobile phones and devices will be switched off or switched to ‘silent’ mode and kept in locker area;
- Staff should not use personal devices such as mobile phones, iPads or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy disciplinary action may be taken.

Dissemination and review

- This policy will be stored in Shared Work-Virtual Teaching File under Policies folder;
- The e-Safety Policy will be formally provided and discussed with all members of staff;
- To protect all staff and pupils, the school will implement an Acceptable Use Policy Agreement;
- Up-to-date and appropriate staff training in safe and responsible internet use, both professionally and personally, will be provided for all members of staff;
- Parents’ attention will be drawn to the school e-Safety Policy in newsletters, the school prospectus and on the school website;
- Information and guidance for parents on e-Safety will be made available.

Policy reviewed: January 2018
Interim Review : Spring 2019 (Carolyn Vagg)
ICT leader: Jesus Jimenez Gazquez