Newton Westpark Primary School

E-Safety Policy

Dated September 2018

Signed……..

Date: ……

Review date: September 2019 and annually there after.

Produced following guidelines provided by Wigan Safeguarding Children Board dates February 2013

Introduction

Headteachers and governing bodies have a legal responsibility to safeguard children and staff and this includes online activity.

In today's society, children, young people and adults interact with technologies such as mobile phones, games consoles and the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial to all, but can occasionally place children, young people and adults in danger.

e-Safety 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 technologies, both in and out of school. It includes education for all members of the school community on risks and responsibilities and is part of the 'duty of care' which applies to everyone working with children.

Purpose

Schools and Early Years Settings and other settings must decide on the right balance between controlling access to the internet and technology, setting rules and boundaries and educating students and staff about responsible use. Schools and Early Years Settings must be aware that children and staff cannot be completely prevented from being exposed to risks both on and offline. Children should be empowered and educated so that they are equipped with the skills to make safe and responsible decisions as well as to feel able to report any concerns. All members of staff need to be 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.

Scope

This e-Safety policy sets out how the school plans to develop and establish its e-Safety approach and to identify core principles which all members of the school community need to be aware of and understand.

The school has appointed an e–Safety Coordinator- **Miss Cliff**

- The e–Safety Policy and its implementation will be reviewed annually.
- Our e–Safety Policy has been written by the school, building on the Wigan e–Safety Policy template and government guidance.
- Our School Policy has been agreed by the Senior Leadership Team and approved by governors.

Contents

1) How will Internet access be authorised

The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.
All staff will read and sign the 'Staff Code of Conduct' and/ or
School Acceptable Use Policy before using any school ICT resources.

- Parents will be asked to read the School Acceptable Use Policy for pupil access and discuss it with their child, where appropriate.
- All visitors to the school site who require access to the Schools and Early Years Settings network or internet access will as part of their induction, be advised of the policy.
- Parents will be informed that pupils will be provided with supervised Internet access appropriate to their age and ability.
- When considering access for vulnerable members of the school community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the pupil(s).

Setting

At Key Stage 1 pupils' access to the Internet will be by adult demonstration with occasional directly supervised access to specific and approved online materials.
At Key Stage 2 pupils will be supervised. Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary.

Risk Assessment

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor Wigan Council can accept liability for the material accessed, or any consequences resulting from Internet use.
The school will use eSafety monitoring software and audit ICT use by staff and pupils/students on a regular basis to establish if the e–Safety policy is adequate and that the implementation of the e–Safety policy is appropriate.
The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Gtr Manchester Police.
Methods to identify, assess and minimise risks will be reviewed regularly.

How will the school respond to any incidents of concern

All members of the school community will be informed about the procedure for reporting e-Safety concerns (such as breaches of filtering, cyberbullying, illegal content etc).

- The e-Safety Coordinator reviews **a system called Impero** and will record all reported incidents and actions taken in the School e-Safety incident log and in other any relevant areas e.g. Bullying or Child protection log.
- The Designated Child Protection Coordinator and other appropriate member of staff will be informed of any e-Safety incidents involving Child Protection concerns,

which will then be escalated appropriately.
- The school will manage e-Safety incidents in accordance with the school discipline/behaviour policy where appropriate.
- The school will inform parents/carers of any incidents of concerns as and when required.
- After any investigations are completed, the school will debrief, identify lessons learnt, implement any changes required, and notify the governing body.
- Where there is cause for concern or fear that illegal activity which concerns an adult has taken place or is taking place then the school will contact the WSCB LADO and Wigan Council HR and OD service so that the incident may be escalated to the Police.
- Where there is cause for concern that a child is at risk of significant harm the school will contact the Central Duty Team.

How will e-Safety complaints be handled

Complaints about Internet misuse will be dealt with under the School's complaints procedure.
Any complaint about staff misuse will be referred to the head teacher. All e–Safety complaints and incidents will be recorded by the school, including any actions taken.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with the school to resolve issues.
- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
- Any issues (including sanctions) will be dealt with according to the school's disciplinary, behaviour and child protection procedures.
- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.

How is the Internet used across the community.

- The school will be sensitive to Internet-related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.
- The school will provide appropriate levels of supervision for students who use the internet and technology whilst on the school site.

.

How will Cyberbullying be managed

Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour.
- There are clear procedures in place to support anyone in the school community affected by cyberbullying.
- All incidents of cyberbullying reported to the school will be recorded.
- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.

- The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the school's e-Safety ethos.

How will mobile phones and personal devices be managed

The use of mobile phones and other personal devices by staff in school will be decided by the school and covered in the school code of conduct.

- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school discipline/behaviour policy.
- Mobile phones and personal devices will be used in line with the school policy.
- Electronic devices of all kinds that are brought in to school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items.

Pupils Use of Personal Devices

- Pupils are not permitted to bring mobile phones into school. If a pupil is found to have one in their possession then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents/carers at the end of the school day..

Staff Use of Personal Devices

- Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.
- Staff will be issued with a school phone where contact with pupils or parents/carers is required.
- Mobile Phone and devices will be used in line with the school policy.
- If members of staff have an educational reason to allow children to use mobile phones or personal device as part of an educational activity then it will only take place when approved by the Senior Leadership Team.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose, unless as part of an approved off-site educational activity with permission from the SLT.
- If a member of staff breaches the school policy then disciplinary action may be taken.

Communication Policy

How will the policy be introduced to pupils

All users will be informed that network and Internet use will be monitored.

- An e–Safety training programme will be established across the school to raise the awareness and importance of safe and responsible internet use amongst pupils.
- Pupil instruction regarding responsible and safe use will precede Internet access.
- An e–Safety module will be included in the PSHE, Citizenship and/or Computing programmes covering both safe school and home use.
- As part of our scheme of work, each year group will be taught a unit on e-Safety.
- Termly e-Safety assemblies will be led by an SLT member.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.
- Particular attention to e-Safety education will be given where pupils are considered to be vulnerable.
- An acceptable use policy for Key Stage 1 and Key Stage 2 pupils will be shared and teachers will sign the policy to say that everyone in their class has read and understood it.
- Pupils will be requested to sign an e–Safety/Internet agreement as part of the Home School Agreement..

How will the policy be discussed with staff

The e–Safety Policy will be formally provided to and discussed with all members of staff. To protect all staff and pupils, the school will implement Acceptable Use Policies.

- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- 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.
- Staff who manage filtering systems or monitor ICT use will be supervised by the Senior Leadership Team and have clear procedures for reporting issues.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

How will parents' support be enlisted

Parents' attention will be drawn to the school e–Safety Policy.

- Parents will be requested to sign an e–Safety/Internet agreement as part of the Home School Agreement..
- Information and guidance for parents on e–Safety will be made available to parents in a variety of formats.
- Advice on useful resources and websites, filtering systems and educational and leisure activities which include responsible use of the Internet will be made available to parents.

Teaching and learning

Why is Internet use important

The rapid developments in electronic communications are having many effects on society. It is important to state what we are trying to achieve in education through ICT and Internet use.

- Internet use is part of the statutory curriculum and is a necessary tool for learning.
- The Internet is a part of everyday life for education, business and social interaction.
- The school has a duty to provide students with quality Internet access as part of their learning experience.
- Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.
- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.
- Internet access is an entitlement for students who show a responsible and mature approach to its use, sanctions will be imposed where Acceptable Use conditions have been breached.
- Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.
- Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and ability.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.
- Pupils will use age-appropriate tools to research Internet content.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

Managing Information Systems

How will information systems security be maintained

It is important to review the security of the whole system from user to Internet. This is a major responsibility that includes not only the delivery of essential learning services but also the personal safety of staff and pupils.

- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Personal data taken off site will be encrypted/protected.
- Portable media may not used without specific permission followed by an anti-virus / malware scan.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the school's network will be regularly checked.
- The ICT coordinator/network manager will review system capacity regularly.

- The use of user logins and passwords to access the school network will be enforced.

How will email be managed

- Staff will only use official school provided email accounts to communicate with pupils and parents/carers, as approved by the Senior Leadership Team.
- Access in school to external personal email accounts may be blocked.
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be.
- Schools and Early Years Settings will have a dedicated email for reporting wellbeing and pastoral issues. This inbox will be managed by designated and trained staff.
- Staff should not use personal email accounts during school hours or for professional purposes.

How will published content be managed

The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information must not be published.

- Email addresses will be published carefully online, to avoid being harvested for spam
- The head teacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.
- The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

Can pupils' images or work be published

Still and moving images and sound add liveliness and interest to a publication, particularly when pupils can be included. Nevertheless the security of staff and pupils is paramount

- Pupils' 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 images/videos of pupils are electronically published.
- Pupils work can only be published with their permission or the parents.
- Written consent will be kept by the school where pupils' images are used for publicity purposes, until the image is no longer in use.

How will social networking, social media and personal publishing be managed

The school will control access to social media and social networking sites.

- Pupils will be advised never to give out personal details of any kind which may identify them and / or their location.
- Staff official blogs or wikis should be password protected and run from the school website with approval from the Senior Leadership Team.
- All members of the school community are advised not to publish specific and

detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
• Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers.
• Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school Acceptable Use Policy and code of conduct.

How will filtering be managed

- The school's broadband access will include filtering appropriate to the age and maturity of pupils.
- The school will ensure that filtering policy is continually reviewed.
- The school will have a clear procedure for reporting breaches of filtering. All members of the school community (all staff and all pupils) will be aware of this procedure.
- The School filtering system will block all sites on the Internet Watch Foundation (IWF) list.
- The School Senior Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective.

How are emerging technologies managed

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Pupils will be instructed about safe and appropriate use of personal devices both on and off site in accordance with the school policy

How should personal data be protected

Personal data will be recorded, processed, transferred and made available according to the GDPR 2018

Appendix 1

added December 2017

Guidance issued by the DfE on: **Sexual violence and sexual harassment between children in schools and colleges**

Sexual Harassment and Sexual Violence Advice.pdf

https://www.gov.uk/government/publications/sexual-violence-and-sexual-harassment-between-children-in-schools-and-colleges

click on either of the links to open)