John Watson School **Wheatley Nursery School**

Acceptable Use of the Internet Policy

Lynn Wong
Signed by Chair of Governors

Date: October 2021

Review Date: October 2022

This policy will be reviewed as per the review schedule set by the Governing body or in accordance with policy updates issued by Oxfordshire County Council (whichever is sooner).

This aims of this policy are:

- to identify the specific risks pertaining to John Watson School staff, students and families,
- to clarify safe practice
- to outline procedures in the event of unsafe practice or a breach of protocol.

For clarity, the e-safety policy uses the following terms unless otherwise stated:

Users - refers to staff, governing body, school volunteers, students and any other person working in or on behalf of the school, including contractors..

Parents – any adult with a legal responsibility for the child/young person outside the school e.g. parent, guardian, carer.

School – any school business or activity conducted on or off the school site, e.g. visits, school trips etc.

Wider school community – students, all staff, governing body, parents, carers, therapists.

Roles and Responsibilities

Governing Body

The governing body will:

- Review this policy at annually and in response to any e-safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure e-safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.
- Ensure the Safeguarding governor has e-safety within their remit and reports incidents to the governing body.

Designated Safeguarding Lead

The Designated Safeguarding Lead will:

- have a lead for e-safety within their remit. This can be delegated to another member of staff (e.g. the ICT Lead within the school) but all incidents must be reported to the Designated Safeguarding Lead via the school Record of Concern system
- follow all incidents up appropriately and will share with the Headteacher and Governors and share the outcome with the person who reported the incident and with all parties concerned
- report incidents to the LADO (Local authority designated officer) and CEOP (Child exploitation and online protection) as appropriate
- ensure the member of staff with the lead for ICT devises a whole school programme for e-safety, teaching our students the risks and strategies for safe use of the internet and how to report to CEOP either themselves, or through a responsible adult, should the need arise
- ensure the member of staff with a lead for ICT offers training to staff and parents on safe use of the internet and how to report incidents to CEOP as necessary
- ensure all staff are clear on the reporting procedure
- review the e-safety policy in the event of e-safety incidents

ICT Technical Support Staff

Technical support staff are responsible for ensuring that the IT technical infrastructure is secure. Technical Support is offered through 123 ICT on the Primary site and Wheatley Park School on the Secondary site. This support will include at a minimum:

- anti-virus software is fit-for-purpose, up to date and applied to all capable devices
- operating system updates are regularly monitored and devices are updated as appropriate

- any e-safety technical solutions such as Internet filtering are operating correctly.
- filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the Designated Safeguarding Lead.
- passwords are applied correctly to all users regardless of age. Passwords for staff will be a minimum of 8 characters.

All Staff
Staff are to ensure that:

- all details within this policy are understood and followed. If anything is not understood it should be brought to the attention of the Designated Lead for Safeguarding.
- any e-safety incident is reported to the Designated Lead for Safeguarding, or in their absence to their line manager.
- any breaches of the acceptable use agreement may be lead to disciplinary action.

All Students
The risks to our students are different to those in mainstream schools. A number of our students are unable to access the internet independently and it is important that staff and family members/carers, accessing it on their behalf are clear as to the risks. As a result, it is not expected that all students sign an acceptable use policy as is the case in most schools, instead, an 'Advice to Parents' sheet (appendix 1) is sent home and parents are asked to sign and all students undergo an 'acceptable use of the internet' lesson at the start of each year.

An acceptable use of the internet policy is shared with all students and their parents/carers, signed and returned. For those students who are unable to use the internet independently, their parents/carers sign to show their understanding of acceptable use.

Technology

John Watson School uses a range of devices including PCs, laptops, Apple Macs, iPads. In order to safeguard the student and in order to prevent loss of personal data we employ the following assistive technology:

Internet Filtering –
Email Filtering
Passwords –
Anti-Virus software

Safe Use

Internet - We believe the internet is a valuable learning tool. It also comes with risks and we will ensure all students able to access the internet independently are taught how to stay safe through the curriculum.

Email – Staff emails are subject to Freedom of Information requests. If it is necessary to send a personal email, it must be marked 'personal' in the subject box in line with county council policy.

Photos and videos – Due to the level of personal care carried out by staff, use of phones with cameras are not permitted in personal care areas, or general areas on site. In designated areas such as offices, team rooms and staff rooms, mobile phone use is permitted. This recognises the need for staff located on both sites to communicate across the school at all times. All parents must sign a photo/video release slip at the beginning of each academic year; non-return of the permission slip will not be assumed as acceptance. Photographs and video should only be taken using school equipment, and not members of staff's own personal devices.

Social Networking -
Out of school, staff using social networking for personal use should never undermine the school, its staff, parents or children. The school, or any obvious reference to it, should not be mentioned on social media. The following guidance prevents staff becoming vulnerable to allegations:

- **Staff should not become "friends" with parents or pupils on personal social networks**.
- The school advises against online friendships and communication with former pupils, particularly if the pupils are under the age of 18 years. In cases where employees in schools/services are related to parents/carers and/or pupils or may have formed online friendships with them prior to them becoming parents/carers and/or pupils of the school/service, they must avoid all reference to school/students and staff on-line.
- Disciplinary action may be taken in relation to those members of staff who choose not to follow the specific guidance outlined above.

The school website
The school website is a broadcast service and a one-way communication method in order to share school information with the wider school community and as such no two-way communication will take place.

In addition, the following is to be strictly adhered to:

- Permission slips (via the school photographic policy) must be consulted before any image or video of any child is uploaded.
- There is to be no identification of students using first name and surname; first name only is to be used.
- All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner's permission has been granted or there is a licence which allows for such use (i.e. creative commons).

Notice and take down policy – should it come to the school's attention that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed within one working day.

Further e-safety information and advice can be found on:

Action for Children Go to http://www.actionforchildren.org.uk/
Chatdanger - potential dangers on interactive services Go to http://www.chatdanger.com/
Child Exploitation and Online Protection Centre Go to http://www.ceop.gov.uk/
Childnet - Internet safety resources Go to http://www.childnet-int.org/kia
Confidential advice Go to http://www.swgfl.org.uk/services
Get safe online Go to http://www.getsafeonline.org/
Kidsmart - internet safety programme Go to http://www.kidsmart.org.uk
ThinkUKnow

Appendices

Appendi 1:

Dear Parents and Carers

At John Watson School, we believe the internet is a valuable tool for learning and can make a useful contribution to home and school work. It does not, however, come without risk and as a result, we have put together the following guidance for home use to reinforce the expectations at school. Please could you sign and return the attached slip to indicate your agreement and to identify any further support you feel you may need.

In line with national guidance, we parents and carers of those able to access the internet independently, we recommend:

- Parents and carers discuss the rules for using the Internet and decide together when, how long, and what comprises appropriate use.
- All devices with internet access are kept in a public space within the home.
- Parents and carers get to know the sites their child visits, and talk to them about what they are learning.
- Parents and carers ensure their child is not giving out personal identifying information on the Internet, such as a picture, an address, phone number, school name,, in any electronic communication.
- Parents/carers do not have financial details saved in devices at home that may enable their child to accidentally buy further levels/opportunities from gaming sites and or buy products in general.
- Parents and carers should encourage their child not to respond to any uninvited messages and to tell them if they receive any such messages or images, so they can report to CEOP on https://www.ceop.police.uk
- Parents and carers ensure that their child does not knowingly make any malicious comments to or about another child, member of the school staff or the school on any site that may lead to it being in the public domain. The school may choose to report the matter to the police should this happen.

At school, we ensure:

- Students do not have access to any social media sites
- Students do not access any sites that are sexually explicit, violent, put them at risk of radicalisation, or make them vulnerable for other reasons. We have tight filters around inappropriate sites and these are applied by 123 ICT on the primary site and Wheatley Park School on the secondary site.
- Students have an understanding of how to use the internet safely, through explicitly teaching safe use.
- Devices with internet access are not permitted on site and all access to the internet is monitored by staff trained in internet safety.
- Students are always supervised when using the internet.
- Should a student gain access to a social media site from a school device by bypassing systems, the school will take disciplinary action in line with the behaviour policy.

Free advice for parents and carers is available from the following sources:

Parent's Online

Website: www.parentsonline.gov.uk

Parents' Information Network (PIN)

Website:http://www.pin.org.uk

PO Box 16394

London SE1 3ZP

Tel: 0891 633 644

Action for Children Go to http://www.actionforchildren.org.uk/

Chatdanger - potential dangers on interactive services Go to http://www.chatdanger.com/

Child Exploitation and Online Protection Centre Go to http://www.ceop.gov.uk/

Childnet - Internet safety resources Go to http://www.childnet-int.org/kia

Confidential advice Go to http://www.swgfl.org.uk/services

Get safe online Go to http://www.getsafeonline.org/

Kidsmart - internet safety programme Go to http://www.kidsmart.org.uk

ThinkUKnow

If you have any further questions, please do not hesitate to contact me.

Best wishes

Stephen Passey

Headteacher and Designated Safeguarding Lead

I/we have read the above guidance and expectations and agree to work in partnership with school to ensure …….(name of student) uses the internet safely.

I would like the following support from the school in internet safety (please tick as appropriate):

- Training on the risks posed by the internet and how to use it safely _
- Leaflet on the risks posed by the internet and how to use it safely _
- Other suggestions:

---

signed…….date……
……

Appendix 2

Acceptable Use Policy – Staff

Note: All Internet and email activity is subject to monitoring
You must read this policy in conjunction with the e-Safety Policy. Once you have read and understood both you must sign this policy sheet.

Internet access - You must not access or attempt to access any sites that contain any of the following: child abuse; pornography; promoting discrimination of any kind; promoting racial or religious hatred; promoting illegal acts; any other information which may be illegal or offensive to colleagues. Inadvertent access must be treated as an e-safety incident, reported to the e-safety officer and an incident form completed.

Social networking – is not allowed in school unless for professional use using Google+. Staff using social networking for personal use should never undermine the school, its staff, parents or children. Staff should not become "friends" with parents or pupils on personal social networks. The school advises against online friendships and communication with former pupils, particularly if the pupils are under the age of 18 years.

Use of Email – In the rare event staff should need to use their school email address for personal business the emails must be marked 'Personal' in the subject box. Staff should be aware all emails from the school email address are subject to Freedom of Information requests and may not be confidential.

Use of Student names - when referring to students in emails initials must be used to protect confidentiality. Students can only be referred to by their first names on the website.

Passwords - Staff should keep passwords private. There is no occasion when a password needs to be shared with another member of staff or student, or IT support.

Personal Use of School ICT - You are not permitted to use ICT equipment for personal use unless specific permission has been given from the Headteacher who will set the boundaries of personal use.

Images and Videos - You should not upload onto any internet site or service images or videos of yourself, other staff or pupils without consent. This is applicable professionally (in school) or personally (i.e. staff outings).

Use of Personal ICT - use of personal ICT equipment is at the discretion of the Headteacher. Permission must be sought stating the reason for using personal equipment; a risk assessment will be carried out by IT support and the Designated Lead for Safeguarding. Personal ICT equipment (in particular mobile phones) must not be used to take photographs or video in school.

Viruses and other malware - any virus outbreaks are to be reported to the ICT technician as soon as it is practical to do so, along with the name of the virus (if known) and actions taken by the school.

e-Safety – like health and safety, e-safety is the responsibility of everyone to everyone. As such you will promote positive e-safety messages in all use of ICT whether you are with other members of staff or with students.

signed……date……
……..