John Watson School

Acceptable Use of the Internet Policy

Signed by *Lynn Wong*
Chair of Governors

Date: Dec 2022
Review Date: Dec 2025

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).

Acceptable Use of the Internet Policy

At John Watson School (JWS), we recognise the importance of safeguarding all pupils.

Our Core Values **SLICE** underpin all learning and ensures a whole school approach to improving the outcomes of pupils

Safety	Learning	Independence	Communication	Engagement

The aims of this policy are to:

- 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 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 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:

- Oxfordshire website: Internet safety and cyberbullying
- Thinkuknow - CEOP tailored to different age groups and for parents and carers
- Disrespectnobody - Home Office advice on healthy relationships
- UK Safer Internet Centre - UK Safer Internet Centre Professional helpline 08443814772
- SWGfL - digital literacy curriculum, e-safety self-assessment tool
- Internet Matters - help for parents and carers on how to keep their children safe online
- ParentZone - help for parents and carers on how to keep their children safe online
- Childnet Cyberbullying - guidance on cyberbullying
- UKCIS - UK Council for Internet Safety
- PSHE Association - NSPCC advice for schools and colleges
- Net-aware - NSPCC advice for parents and carers
- Commonsensemedia - information and reviews on all types of media for children and parents and carers
- LGfL - advice from the London Grid for Learning
- Anti-Bullying Alliance - resources from the Anti-bullying Alliance
- Get safe online - internet and online safety