Rednock School

Quality, Partnership, Success

E-mail: admin@rednockschool.org.uk
www.rednockschool.org.uk

Proposed Policy:	Online Safety	Responsibility Of:	Demelza Barker
Date of Ratification:	December 2021	Date of Review:	December 2022

ONLINE SAFETY POLICY

RATIONALE

New technologies have become integral to the lives of young people both within school and in their lives outside of school. The internet and other technologies are powerful tools, which open up new opportunities. Electronic communication promotes effective teaching and learning through the multiplicity of digital and information applications. All young people should have an entitlement to access such technologies, to enhance motivation and engagement and thus facilitate continued improvements in standards across all curriculum areas.

The requirement to ensure that young people are able to use technologies appropriately and safely, should be addressed as part of the wider duty of care to which all those who work in schools are bound.
This Online Safety policy should ensure safe and appropriate use. The implementation of this strategy involves all stakeholders in the school community.

PURPOSE

The use of these new technologies can put young people at risk therefore this policy addresses some of the dangers they may face, including:

- Access to illegal, harmful or inappropriate images
- Unauthorised access to, or loss of, or inappropriate sharing of personal information
- Access to harmful websites, for example those devoted to weapons production, how to take one's own life or promoting high risk behaviours
- The risk of being subject to grooming via the internet, and possibly meeting high risk individuals off line
- The sharing and/or distribution of personal images without the individuals consent or knowledge
- Inappropriate communication with others including strangers
- Cyber bullying
- Access to unsuitable video/internet games
- The inability to evaluate the accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of files
- The potential for excessive/obsessive use

This list is not intended to be exhaustive.

This Online Safety policy should be used in conjunction with all other child protection and Safeguarding policies. The aim of the Online Safety policy should be to build a student's resilience to risk through good educational provision. The school must provide the necessary safeguards to help ensure that everything that could reasonably be expected of the organisation has been done to manage and reduce risk.

GUIDELINES

Education & Training

- It is essential that all users of the network receive Online Safety training and understand their responsibilities. Children and young people need the help and support of the school to recognise and avoid Online Safety risks and build their resilience.

- The DSL/DDSL will attend regular Online Safety training and provide training and advice for members of students, staff and governors.

- Students will receive formal Online Safety training through ICT lessons, Skills Based Curriculum and Life Skills Programme, using the CEOP Think you Know materials, Crag-Rats presentations in assemblies and tutor activities. Online Safety messages will be reinforced through ICT across the curriculum.

- The school will provide information and awareness to parents and carers through seminars at Open Evenings and Parents' Consultation sessions, the school website and social media.

Technical – infrastructure / equipment, filtering and monitoring

- The school's ICT system is managed to ensure that the school meets the Online Safety technical requirements outlined in the SWGfL Security Policy.

- The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so. Rednock School automatically receive the benefits of the SWGfL managed filtering service. The responsibility for the management of the school's filtering policy will be held by the IT Manager. As a further preventative measure, the school will offer advice to parents and students about safe use of the Internet, although it is not the responsibility of the school to control/manage use of the internet at home. The school will work in partnership with parents to ensure that children are as safe as possible whilst using the internet.

Internet monitoring procedures

- We have the ability to use monitoring software, which identifies and logs any inappropriate internet activity, where there is reasonable cause.

- Any teacher who suspects a child is accessing inappropriate material can request an activity report, or use the Impero Console software to monitor use, live in the classroom. If there is cause for concern, this is dealt with in accordance with the standard behaviour procedures. Serious incidents are dealt with by the Designated Safeguarding Lead/Deputy DSL, SLT / Headteacher (depending on seriousness). Sanctions will be used according to the severity of the offence and/or safeguarding procedures followed.

Checking procedures

- If staff need to check a student's internet activity then the request must be made via the Helpdesk system (so the request is recorded/trackable)
- IT Support staff will check the logs and respond via the Helpdesk.
- If the request relates to safeguarding the IT Support staff will also inform the relevant CL
- The CL will ensure the DSL is informed of any internet use which may affect the safety or well-being of any student.

Acceptable Use Policies

The school will try to ensure that all users will have good access to ICT to enhance their work, to enhance learning opportunities and will, in return, expect students, staff and volunteers to agree to be responsible users. All users are provided with a username and strong password by the ICT system Administrators when they have signed the appropriate Acceptable User Policy.

Acceptable Use Policy is intended to ensure:

- All users will be responsible and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

- That school ICT systems and users are protected and risk is minimised from accidental or deliberate misuse that could compromise the security of the systems and users.

- That parents and carers are aware of the importance of Online Safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

- That parents and carers understand that digital images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school.

- That parents and carers agree that if they take digital or video images at, or of, – school events which include images of children, other than they own, that they will abide by the school guidelines in the use of these images.

Students using mobile devices in school

The use of mobile phones in school is not permitted for years 7-11. Sixth form students may use their mobile phones in designated areas during social time or for school work purposes (see Mobile Phone Policy).

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

Use of digital and video images - Photographic, Video

Students and Staff take and use digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. **Those images should only be taken on school equipment.**

Written permission from parents or carers and students will be obtained on an 'opt in' basis before photographs of students are published on the school website or used for publicity that reasonably celebrates success and promotes the work of the school. Consent is requested on our admission form, which is sent to all new applicants before their admission to Rednock. A data collection sheet is sent to all students annually, where parents/carers can review that consent and amend if required.

Communications

Students are provided with individual school Gmail addresses for educational use and must immediately report, to a teacher if they receive any email that makes them feel uncomfortable, is suspicious, offensive, threatening or bullying in nature and must not respond to any such email.

Any communication between staff and students or parents / carers via email must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not, under any circumstances, be used for these communications.

Students and staff should not engage in social conversations with each other via email, text or social networking sites such as Facebook. Users need to be aware that email communications may be monitored.

Responding to incidents of misuse

It is anticipated that all members of the school community will be responsible users of ICT, however, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

There will be no tolerance of cyber-bullying

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal it is essential to report it to the relevant Community Leader as soon as possible and it will be dealt with through normal behaviour / disciplinary procedures (see Anti-bullying and Behaviour for Learning policies).

If any apparent or actual misuse appears to involve illegal activity the school will follow the SWGfL guidance and flow chart – this will also involve intervention from the IT Manager and Head Teacher, as necessary.

The school will monitor the impact of the policy using the SWGFL, and internal logging of incidents on SIMS, and by surveying students, parents and staff.

Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Arrangements for monitoring & evaluation of this policy

- Designated Safeguarding Lead or deputy in her absence will cross-reference Child Protection Policy with all other associated policies as listed in the Report to Governing Body on Safeguarding Children.
- Governor responsible for Child Protection (Jane Barker-Doe) will review all processes on an annual basis.

Related policies/documents (this list is not exhaustive):

- Social media policy
- Mobile phone policy
- Anti-bullying policy
- Behaviour management policy
- Child protection (safeguarding policy)
- Student ICT acceptable use statement
- Staff ICT acceptable use policy

Addendum – Staff Use of Social Media

RATIONALE

We recognise that staff will use online and digital technologies in their personal and social lives. We do not seek to prevent any member of staff from accessing online technologies. However, we do ask that every member of staff adhere to the Teachers' Standards in England from September 2012, Part Two: 'Personal and Professional Conduct', and at all times observe proper boundaries appropriate to a teacher's professional position; ensuring there is no confusion between their personal and professional roles.

Staff at Rednock must agree that through their recreational use of social networking sites or other online technologies they should:

- Not bring Rednock School into disrepute.
- Observe confidentiality and refrain from discussing any issues relating to work, children or parents/carers.
- Not share or post, in an open forum, any information that I would not want children, parents/carers or colleagues to view.
- Set privacy settings to block unauthorised access to my page and to restrict those who are able to receive updates.
- Keep professional and personal life separate, and will not accept children and parents/carers as 'friends'.
- Consider how social conduct may be perceived by others and how this could affect their own reputation and that of the school.
- Either avoid using a profile photograph or ensure it is a respectable image that staff would be happy to share with anyone.
- Report any known breaches of the above.

In addition to the above, the following guidelines are intended not as a set of instructions, but general advice on how to avoid compromising your professional position. These guidelines are also agreed and issued by NASUWT.

Privacy

- Ensure that your Social Networking account(s) does/ do not compromise your professional position, please ensure that your privacy settings are set correctly.
- Do not under any circumstances accept friend requests from a person you believe to be either a parent or a pupil at Rednock School.

As a minimum, Rednock School recommends the following:

Privacy Setting Recommended security level:

Send you messages Friends only
See your friend list Friends only
See your education and work Friends only
See your current city and hometown Friends only
See your likes, activities and other connections Friends only
Your status, photos, and posts Friends only
Bio and favourite quotations Friends only
Family and relationships Friends only
Photos and videos you're tagged in Friends only
Religious and political views Friends only
Birthday Friends only
Permission to comment on your posts Friends only
Places you check in to Friends only
Contact information Friends only

- Always make sure that you log out of Social Networking accounts, particularly when using a shared machine. Your account can be hijacked by others if you remain logged in – even if you quit your browser and/or switch the machine off. Similarly, Facebook's instant chat facility caches conversations that can be viewed later on. Make sure you clear your chat history on Facebook (click "Clear Chat history" in the chat window).
- Employers may scour websites looking for information before a job interview. Take care to remove any content you would not want them to see.

Conduct on social networking sites

- Do not make disparaging remarks about Rednock School or individual colleagues. Doing this in the presence of others may be deemed as bullying and/or harassment.
- Other users could post a photo on their profile in which you are named, so think about any photos you appear in. On Facebook, you can 'untag' yourself from a photo. If you do find inappropriate references to you and/or images of you posted by a 'friend' online you should contact them and the site to have the material removed.
- Parents and students may access your profile and could, if they find the information and/or images it contains offensive, complain to your employer.
- If you have any concerns about information on your social networking site or if you are the victim of cyberbullying, you should contact your Head Teacher and Union Regional Centre immediately.
- Do not publish your date of birth and home address on Facebook. Identity theft is a crime on the rise with criminals using such information to access to your bank or credit card account.
- Stop the network provider from passing on your details to other companies for research and advertising purposes. For example, to stop Facebook from forwarding your details, click "Privacy Settings". Under "Applications and websites" click "edit your settings". Scroll down to "instant personalisation" and make sure the checkbox for "enable instant personalisation on partner websites" is unchecked.
- Ensure that any comments and/or images could not be deemed defamatory or in breach of copyright legislation.