NEWLANDS GIRLS' SCHOOL

POLICY DOCUMENT

Online Safety Policy

POLICY TYPE	Voluntary/School Policy
REVIEW DATE	Annually – July 2024

RESPONSIBLE		
Leadership Team	Deputy Headteacher – Andrew Morbey	
Governing Committee	School Policy	
APPROVED:	Minuted approval at	Governors Meeting
	Meeting Date	10th July 2023

COURAGE COMMITMENT COMPASSION

Contents

---

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

Unacceptable content is any content that falls into these categories of risk.

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools

- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 Governors

The Governing Board has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

All Governors will:

- Ensure that they have read and understand this policy
- Appoint a Governor with responsibility for working with the school to ensure all filtering and monitoring standards are met.
- Review the school's filtering and monitoring standards annually.
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2)

3.2 The Headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The Designated Safeguarding Lead

Details of the school's Designated Safeguarding Lead (DSL) and Deputies are set out in our Child Protection and Safeguarding policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Headteacher, Deputy Headteacher with responsibility for IT Strategy, Systems Manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Ensuring online safety is part of regular staff training
- Liaising with other agencies and/or external services if necessary
- Reviewing filtering and monitoring logs
- Determining the filtering to be used and ensuring that it does not unreasonably impact teaching and learning

3.4 The Network Systems Manager

The Network Systems Manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- Ensuring that while filtering and monitoring is in place, it should not unreasonably impact teaching and learning or restrict students from learning how to assess and manage risks themselves.
- Regularly preparing and passing on monitoring reports to the SLT and DSL as required.
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a regular basis
- Blocking access to potentially dangerous sites that are identified and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any incidents of cyber-bullying are dealt with appropriately by passing them on to the DSL or relevant Head of Year

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Working with the DSL to ensure that any online safety incidents are reported and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'
- Reporting any of the following concerns using CPOMS:
    - See or suspect unacceptable content is being accessed
    - Discovering unacceptable content can be accessed
    - Teaching content that could see a spike in logs
    - Failure or abuse of the system
    - Perceived unreasonable restrictions
    - Abbreviations or misspellings that could allow access to unacceptable content

3.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre

- Hot topics – Childnet International
- Parent resource sheet – Childnet International

4. Educating pupils about online safety

Pupils will be taught about online safety as part of our curriculum which has been developed using guidance on relationships education, relationships and sex education (RSE) and health education.

Online safety is taught through the PSHE and Pastoral Personal Development curriculum, the assembly programme and Computing lessons.

In **Key Stage 3**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- The legal aspects of online safety.
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the **end of secondary school**, pupils will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in Newlands News and other communications home, at parent information evenings and in information on our website. This policy will also be shared with parents.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Form Tutor or Head of Year.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social media sites, email, instant messaging services, online gaming or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teachers will discuss cyber-bullying with their tutor groups.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 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, tablets, and other portable 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 the material, or
- Retain it as evidence (of a possible criminal offence* or a breach of school discipline), and/or
- Report it to the police

Staff will also confiscate the device to give to the police, if they have reasonable grounds to suspect that it contains evidence in relation to an offence.

If a staff member **believes** a device **may** contain a nude or semi-nude image or an image that it's a criminal offence to possess, they will not view the image but will report this to the DSL immediately, who will decide

what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people.

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

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

7. Acceptable use of the internet in school

All pupils, parents and staff, are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 to 3).

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements found on the school website.

8. Pupils using mobile phones and devices in school

Pupils may bring mobile phones into school but are not permitted to use them during the school day unless they are in the Sixth Form.

The sight and sound of a mobile phone being used will result in confiscation of the device in line with the school's Behaviour Policy and Behaviour Principles. This also applies to other mobile devices such as tablets and laptops.

Smart watches are allowed to be worn however they must not be used for any purpose other than displaying the time while in school.

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Not sharing their password with others
- Not using portable hard disk drives or USB storage devices
- Not leaving the device unlocked while unattended
- Not sharing the device among family or friends

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2.

Work devices must be used solely for work activities.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on Behaviour, and Home/School agreement. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems, access to the internet or other networks, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, harassing, and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and Deputy DSLs will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Links with other policies

This online safety policy is linked to our:

- Child protection (Safeguarding) policy
- Behaviour policy
- Staff Code of Conduct
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy
- Home/School Agreement

Appendix 1

NEWLANDS GIRLS' SCHOOL

INFORMATION TECHNOLOGY

ACCEPTABLE USE AGREEMENT - INCLUDING ADVICE TO PARENTS

The school uses Information Technology equipment to support the curriculum and help girls extend their learning both inside and outside the classroom. Access to this equipment and these resources is a privilege which, in the event of improper use, can be withdrawn.

Please read the following sections carefully:

Equipment use in school

- Only use the computers for educational purposes
- Damaging, disabling, or otherwise harming the operation of computers, or intentionally wasting resources puts your work at risk, and will cut short your time with the IT equipment.
- If permitted, always check mobile equipment (e.g. laptops, tablet PCs, smartphones etc.) with antivirus software and ensure they have been found to be clean of viruses before connecting them to the network. Always check files brought in on removable media (CDs, flash drives etc.) with antivirus software and only use them if they are found to be clean of viruses. It is students' responsibility to keep antivirus software up to date.
- Eating and drinking is expressly forbidden in any of the computer rooms, and in any rooms where computer equipment is to be used.

Security and Privacy

- Your student login details (username and password) are your own personal property and you are responsible for keeping them private and secure. Use them to protect your work and your email account; do not share them with anybody and never use someone else's login.
- Always be wary about revealing any personal information including your home address, telephone number, school name, or picture on the Internet.
- Once logged on, store only your own work on your area; do not store work or files for anybody else, or allow them to store work or files for you.
- To protect yourself and the systems, you should respect the security on the computers;

attempting to bypass or alter the settings may put you, your work, or other girls at risk.

- Computer storage areas will be treated like school lockers. Your computer use may be reviewed by appropriate staff members to ensure that you are using the system appropriately, safely and responsibly.

- Other computer users should be respected and should not be harassed, harmed, offended or insulted.
  .

Internet/Intranet (general advice)

- You should only access the Internet/Intranet for school activities.

- Only access suitable material; using the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive is not permitted.

- Respect the work and ownership rights of people outside the school, as well as other students or staff. This includes abiding by copyright laws.

- People you contact on the Internet are not always who they seem. You should never meet with anyone contacted through the internet.

Email/Messaging (general advice)

- Cyber bullying is dealt with in the same was as any other incident of bullying and is not tolerated at Newlands. Messages sent between students outside school hours still constitute bullying.

- Emails and Teams messages are able to be seen by the IT manager and Leadership Team. You should only send messages that you would be happy for your parents or carers to see.

- Be polite and appreciate that other users might have different views from your own. The use of strong language, swearing or aggressive behaviour is as anti-social on the Internet as it is on the street.

- Only open attachments to emails if they come from someone you already know and trust. Attachments can contain viruses or other programs that could destroy all the files and software on your computer.

- If you receive an email containing material of a violent, dangerous, racist, sexual or inappropriate content, always report such messages to a member of staff/trusted adult **immediately**. The sending or receiving of an email containing content likely to be unsuitable for children or schools is strictly forbidden.

Internet advice for Parents/Carers

- Go online with your child and get involved. Search together for useful websites and get to know what Internet resources your child uses. Learn from your child and get to know their online friends.

- Be proactive and caring and warn your child about the dangers of giving out their name, address, telephone number and any other personal information, whether online or not.

- Discuss family and personal values and devise rules for responsible behaviour. Post the rules by the home computer and check to see if they are complied with. At school, teachers will guide pupils on how to use the internet safely. Outside school, families have the responsibility for such guidance.

- Please be aware that if a pupil uses Social Media platforms to harass, cause significant harm to another individual (outside of school hours) or bring the school into disrepute, we may act in school to address such behaviour and/or involve the police when appropriate.

- It is wise to install filtering software and any parental controls that are provided by many commercial online services, but above all else be vigilant.

  Please sign below and once this is returned to school, access to the Internet will be permitted. If a student violates these provisions, access to the Internet will be denied and disciplinary action will be taken. Additional action may be taken by the school in line with existing policy regarding school behaviour. When appropriate, police or local authorities may be involved.

Appendix 2

NEWLANDS GIRLS' SCHOOL

INFORMATION TECHNOLOGY

ACCEPTABLE USE AGREEMENT FOR STAFF

ICT is an integral part of the way our school works, and is a critical resource for pupils, staff, governors, volunteers and visitors. It supports teaching and learning, pastoral and administrative functions of the school. Allow the school network to safely support teaching and learning and business functions.

Please read the following sections carefully:

Staff will

- Ensure that their use of computer systems is consistent with school policy and the law.
- Not access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Not share their passwords or login details with any other person.
- Not create, upload, download, access or forward any material that is likely to harass, cause offence or anything that could bring the school or their professional role into disrepute.
- Respect copyright and intellectual property rights.
- Not use any improper language when communicating online, including in emails or other messaging services
- Ensure that they keep their school laptop of applicable safely and securely and will ensure that it is not damaged through neglect or mistreatment.
- Not attempt to bypass or alter the security settings.
- Attempt to send as few emails as possible. If possible speak to the member of staff you are wanting to communicate with and only copy in colleagues who need to see the email.
- Be careful when responding to emails that appear genuine. Always report any emails that maybe unsafe eg phishing emails asking for login details or attachments from someone you were not expecting an attachment from. These should be reported to the Network Manager.
- Only open attachments to emails if they come from someone you already know and trust. Attachments can contain viruses or other programs that could destroy all the files and software on your computer.
- Report unacceptable content to the DSL immediately.
- Not share passwords with others or log in to the school's network using someone else's details
- Share confidential information about the school, its pupils or staff, or other members of the community

By signing the 'Safeguarding Updates September 2023' slip, you agree that:

I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.
I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.
I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.
I understand that if I fail to comply with this Guidance and Agreement for the Acceptable use of ICT, I could be subject to disciplinary action. I confirm that, in the case of my needing further clarification on any point, I have consulted a member of the Leadership Team.