NEWPORT GIRLS' HIGH SCHOOL ACADEMY TRUST

ONLINE SAFETY POLICY

Policy written by:	Mrs H Birch
Policy reviewed:	June 2023
Next review due:	June 2024
Statutory Governor Approval:	**July 2023**

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
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

Legislation and Guidance

This policy has been designed following advice and guidance from SWGfL, UK Safer Internet Centre and the NSPCC. It is also informed by the Department for Education's statutory safeguarding guidance 'Keeping Children Safe in Education (updated 2023)' and its advice for schools on 'Preventing and tackling bullying' and 'searching, screening and confiscation'. It also refers to the Department's guidance on 'protecting children from radicalisation'.

It also reflects existing legislation, including the Education Act, the Education and Inspections Act and the Equality Act. This gives teachers stronger powers to tackle cyberbullying by, if necessary, searching for and deleting inappropriate images or files on students' electronic devices where they believe there is 'good reason to do so'.

This policy is linked to our existing policies on Anti-Bullying, ICT Acceptable Use Policy for students and staff, Mobile Phone Policy and Child Protection and Safeguarding Policy. Our school recognises the need to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely. This is addressed as part of our wider duty of care to keep our students safe from harm, this forms part of our safeguarding practices which all teachers and support staff follow.

Due to the ever-changing nature of digital technologies, the school will review the Online Safety Policy annually and, if necessary, more frequently in response to any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place.

The technologies that this policy refers to include websites, email, instant messaging, chat rooms, social media, mobile phones, blogs, podcasts and downloads.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school:

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. The role of Online Safety Governor will include:

- regular meetings with the Child Protection and Safeguarding team about online safety concerns
- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs

All Governors will:

- ensure that they have read and understood this policy

Headteacher and Senior Leadership Team

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Designated Safeguarding Lead who has responsibility for safeguarding and student wellbeing which includes online safety.
- The Headteacher and the Senior Leadership Team are all aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff (see flow chart on dealing with online safety incidents included below – 'Responding to incidents of misuse').
- The Headteacher and Senior Leadership Team are responsible for ensuring that all staff receive suitable training

about online safety.

Designated Safeguarding Lead

Details of the school's designated lead (DSL) and deputies are set out in our child protection and safeguarding policy. The DSL:

- Supports the student led Wellbeing Group.
- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Ensures that filtering and monitoring standards are met and upheld in accordance to the guidance.
- Provides training and advice for staff.
- Liaises with the Local Authority and social care teams.
- Meets regularly with CSE lead.
- Liaises with ICT Services.
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments.
- Meets with Designated Safeguarding Governor to discuss current issues, review incident logs and filtering control logs
- Attends relevant Governors meetings
- Reports to Senior Leadership Team

The DSL is trained in online safety issues and is aware of the potential for serious child protection or safeguarding issues to arise from:

- Sharing of personal data
- Access to illegal / inappropriate materials
- Inappropriate on-line contact with adults / strangers
- Potential or actual incidents of grooming / CSE
- Online-bullying

ICT Services

The ICT Network Manager is responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- That the school meets required online safety technical requirements.
- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- The filtering policy is applied and updated on a regular basis.
- That they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- That the use of the network / internet / remote access / email is regularly monitored in order that any attempted misuse can be reported to the Headteacher or Designated Safeguarding Lead for further investigation.

Teaching and Support Staff

Are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices
- They have read, understood and signed the ICT and Internet Acceptable Use Policy: Staff
- They report any suspected misuse or problem to the Headteacher or Designated Safeguarding Lead for further investigation.
- All digital communications with students, parents / carers should be on a professional level and only carried out using official school systems,
- Online safety issues are embedded in all aspects of the curriculum and other activities.

- Students understand and follow the Online Safety Policy and Acceptable Use Policy.
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement all current school policies with regard to these devices.
- In lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Students:

- Are responsible for using the school digital technology systems in accordance with the ICT and Internet Acceptable Use Policy: Students and Mobile Phone Policy.
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and online bullying.
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions outside of school, if related to their membership of the school.

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. The school will take every opportunity to help parents / carers understand these issues through parents' evenings and Newport News. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website

Educating pupils about online safety

From September 2020 **all** schools will have to teach:

- Relationships and sex education and health education in secondary schools

This new requirement includes aspects about online safety.

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
- 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**, they 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

The safe use of social media and the internet will also be covered in other subjects where relevant and this is shared in the Relationship and Sex Education Policy. The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

Educating Parents / Carers about online safety

The school will raise parents' awareness of internet safety in letters and newsletters and additional information can also be accessed via our website. Online safety will also be covered during parents' welcome evenings annually.

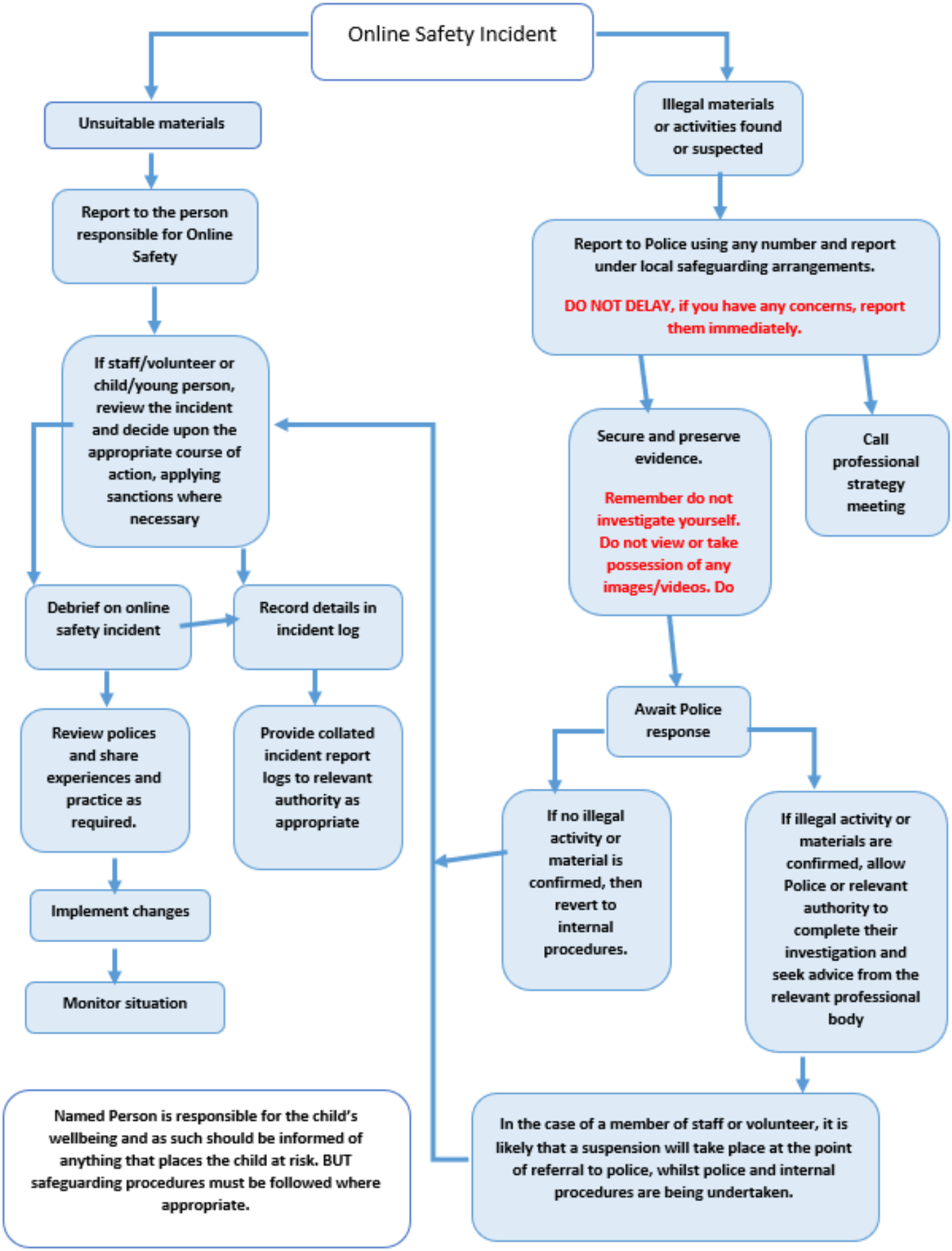
If parents have any queries or concerns in relation to online safety, these should be raised with the students Head of Year who will liaise with the safeguarding team if required. Concerns or queries about this policy can be raised with any member of staff or the headteacher.

Dealing with unsuitable / inappropriate activities

Some internet activity is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities. Any use of these would be dealt with in accordance with the school's behaviour policy.

Responding to incidents of misuse

The school encourages a safe and secure approach to the management of responding to incidents of misuse. Such incidents might involve illegal or inappropriate activities. The school will use the guidance as shown in the flowchart below to manage any incidents that raise a cause for concern.


Online Safety Incident
Unsuitable materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Record details in incident log
Review polices and share experiences and practice as required.
Provide collated incident report logs to relevant authority as appropriate
Implement changes
Monitor situation
Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.
Illegal materials or activities found or suspected
Report to Police using any number and report under local safeguarding arrangements.
DO NOT DELAY, if you have any concerns, report them immediately.
Secure and preserve evidence.
Remember do not investigate yourself. Do not view or take possession of any images/videos. Do
Call professional strategy meeting
Await Police response
If no illegal activity or material is confirmed, then revert to internal procedures.
If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

School Incidents & Sanctions

Schools are more likely to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through our behaviour policy, incidents that would be investigated further are:

- Deliberately accessing or trying to access material that could be considered illegal
- Unauthorised use of non-educational sites during lessons
- Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device
- Unauthorised / inappropriate use of social media / messaging apps / personal email
- Unauthorised downloading or uploading of files
- Allowing others to access the school network by sharing username and passwords
- Attempting to access or accessing the school network, using another student's account
- Attempting to access or accessing the school network, using the account of a member of staff
- Corrupting or destroying the data of other users
- Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature
- Continued infringements of the above, following previous warnings or sanctions
- Actions which could bring the school into disrepute or breach the integrity of the ethos of the school
- Using proxy sites or other means to subvert the school's filtering system
- Accidentally accessing offensive or pornographic material and failing to report the incident
- Deliberately accessing or trying to access offensive or pornographic material
- Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act 2018