



Online Safety

DOCUMENT REFERENCE	Online safety Policy
PUBLICATION DATE	November 2021
AUTHORISING OFFICER	Martyn Henson
AUTHORISING OFFICER'S SIGNATURE	
AUTHOR	Steve Morley
POST	Asst Head
DATE APPROVED BY GOVERNORS	November 2021
AUTHORISING GOVERNOR'S SIGNATURE	
REVIEW DATE	November 2023
TARGET AUDIENCE	All staff, students and parents.
STATUS	Approved

Contents – section

1. Introduction	1
2. Responsibilities	1
3. Scope of policy	1
4. Policy and procedure	2
Use of email	2
Visiting online sites and downloading	2
Storage of Images	4
Use of personal mobile devices (including phones)	4
New technological devices	4
Reporting incidents, abuse and inappropriate material	5
5. Curriculum	5
6. Staff and Governor Training.....	6
7. Working in Partnership with Parents/Carers.....	6
8. Records, monitoring and review.....	6
9. Appendices of the Online Safety Policy.....	7
Appendix A - Guidance on the process for responding to cyberbullying incidents	8
Appendix B - Guidance for staff on preventing and responding to negative comments on social media.....	9
Appendix C - Online safety incident reporting form	11
Appendix D - Online safety incident record	13
Appendix E - Online safety incident log.....	15

1. Introduction

The Nobel School recognises that internet, mobile and digital technologies provide positive opportunities for children and young people to learn, socialise and play but they also need to understand the challenges and risks. The digital world is an amazing place, but with few rules. It is vast and fast moving and young people's future economic success may be partly dependent on their online skills and reputation. We are, therefore, committed to ensuring that **all** pupils, staff and governors will be supported to use internet, mobile and digital technologies safely. This is part of our safeguarding responsibility. Staff are aware that some pupils may require additional support or teaching, including reminders, prompts and further explanation to reinforce their knowledge and understanding of online safety issues.

We are also committed to ensuring that all those who work with children and young people, including their parents/carers, are informed about the ever-changing risks so that they can take an active part in helping children and young people navigate the online world safely and confidently.

2. Responsibilities

The headteacher and governors have ultimate responsibility to ensure that appropriate online safety policy and practice is embedded and monitored. The named online safety lead in this school is Steve Morley.

All breaches of this policy must be reported to him.

All breaches of this policy that may have put a child at risk must also be reported to the DSL, Steve Morley.

Organisations that are renting space from the school and are a totally separate organisation should have and follow their own online safety policy and acceptable use agreements. However, if the organisation has any access to the school network, cloud-based services and/or equipment then they must adhere to the school's online safety procedures and acceptable use agreements.

If the organisation is operating in school time or when pupils are on site in the care of the school, then the safeguarding of pupils is paramount and the organisation must adhere to the school's online safety procedures and acceptable use agreements.

3. Scope of policy

The policy applies to:

- pupils
- parents/carers
- teaching and support staff
- school governors
- peripatetic teachers/coaches, supply teachers, student teachers
- visitors
- volunteers
- voluntary, statutory or community organisations using the school's facilities

The school also works with partners and other providers to ensure that pupils who receive part of their education off site or who are on a school trip or residential are safe online.

The school provides online safety information for parents/carers, through the website, in newsletters and at some events. It is important that parents/carers understand their key role in supporting their child/ren to behave appropriately and keep themselves safe online.

This policy, supported by the schools acceptable use agreements, is intended to protect

the interests and safety of the whole school community. It is linked to the following other school policies and documents: safeguarding, Keeping Children Safe in Education, GDPR, health and safety, home–school agreement, home learning, behaviour, anti-bullying and the RSE policies.

4. Policy and procedure

The school seeks to ensure that internet, mobile and digital technologies are used effectively and safely, for their intended educational purpose, in ways that will not infringe legal requirements or create unnecessary risk.

The school expects everyone to use internet, mobile and digital technologies responsibly and strictly according to the conditions set out in this policy. This policy also includes expectations on appropriate online behaviour and use of technology outside of school for pupils, parents/carers, staff and governors and all other visitors to the school.

Use of email

Staff and governors should use a school email account or MS Teams for all official school communication to ensure everyone is protected through the traceability of communication. Under no circumstances should staff contact pupils, parents or conduct any school business using a personal email address. Pupils should use school approved accounts on the school system for educational purposes. Where required parent/carer permission will be obtained for the pupil account to exist. For advice on emailing, sharing personal or confidential information or the need to gain parent permission refer to the policy for GDPR. Emails created or received as part of any school role will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000.

Staff, governors and pupils should not open emails or attachments from suspect sources and should report their receipt to Mark Smith (IT Network Manager).

Users must not send emails which are offensive, embarrassing or upsetting to anyone (i.e. cyberbullying).

Visiting online sites and downloading

- Staff must, where possible, preview sites, software and apps before their use in school or before recommending them to pupils. Before using any online service that requires user accounts to be created or the sharing of any personal data, staff must consult with the Data Protection Officer with details of the site/service and seek approval from a senior leader. The terms and conditions of the service should be read and adhered to, and parental/carer permission sought where required. If internet research is set for homework, specific sites will be suggested that have been checked by the teacher. All users must observe copyright of materials from electronic sources.
- Staff must only use pre-approved systems if creating blogs, wikis or other online content.
- When working with pupils searching for images should be done through Google Safe Search (standard through the HICS service), Google Advanced Search or a similar application that provides greater safety than a standard search engine.

Users must not:

Visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

- Indecent images of children actually or apparently under the age of 18 or images of child abuse (i.e. images of children, digital or cartoons, involved in sexual activity or posed to be sexually provocative)
- Indecent images of vulnerable people over the age of 18 (i.e. images of vulnerable people, digital or cartoons involved in sexual activity or posed to be sexually provocative)
- Adult material that breaches the Obscene Publications Act in the UK
- Promoting discrimination of any kind in relation to the protected characteristics: age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race or ethnicity, religion or belief, sex, sexual orientation
- Promoting hatred against any individual or group from the protected characteristics above
- Promoting illegal acts including physical or sexual abuse of children or adults, violence, bomb making, drug and alcohol abuse and software piracy
- Any material that may bring the school or any individual within it into disrepute e.g. promotion of violence, gambling, libel and disrespect

Users must not:

- Reveal or publicise confidential or proprietary information
- Intentionally interfere with the normal operation of the internet connection, including the propagation of computer viruses
- Transmit unsolicited commercial or advertising material either to other users, or to organisations connected to other networks except where permission has been given to the school
- Use the school's hardware and Wi-Fi facilities for running a private business
- Intimidate, threaten or cause harm to others
- Access or interfere in any way with other users' accounts
- Use software or hardware that has been prohibited by the school

Only a school device may be used to conduct school business outside of school. The only exception would be where a closed, monitorable system has been set up by the school for use on a personal device e.g. Teams or the school HUB. Such a system would ensure the user was not saving files locally to their own device and breaching data security.

All breaches of prohibited behaviours detailed above will be investigated, where appropriate, in liaison with the police; as required.

The school recognises that in certain planned curricular activities, access to controversial and/or offensive online content may be beneficial for educational use. In such circumstances, there is an expectation that access is pre-planned, risk assessed and recorded, and permission given by Mark Smith (IT Network Manager).

Storage of Images

Photographs and videos provide valuable evidence of pupils' achievement and progress in a variety of contexts and can be used to celebrate the work of the school. In line with GDPR they are used only with the written consent of parents/carers which is secured in the first instance on a child's entry to the school. Records are kept on file and consent can be changed by parents/carers at any time. (See GDPR policy for greater clarification).

Photographs and images of pupils are only stored on the school's agreed secure networks which include some cloud based services. Rights of access to stored images are restricted to approved staff as determined by Steve Morley. Staff and pupils may have temporary access to photographs taken during a class session, but these will be transferred/deleted promptly afterwards.

Parents/carers should note that there may be some children who are at risk and must not have their image put online and others who do not want their image online. For these reasons parents/carers must follow the school's Acceptable Use Agreement and refrain from taking or posting online photographs of any member of the school community, other than their own child/ren.

Staff and other professionals working with pupils, must only use school equipment to record images of pupils whether on or off site. See also GDPR. Permission to use images of all staff who work at the school is sought on induction and a written record is located in the personnel file.

Use of personal mobile devices (including phones) - please also see BYOD Policy 2021

The school allows staff, including temporary and peripatetic staff, and visitors to use personal mobile phones and devices within the school but only as appropriate. Under no circumstance does the school allow a member of staff to contact a pupil or parent/carer using their personal device without the personal phone number being hidden (user ID off, 141 preceding the number).

Parents/carers may use personal mobile phones and devices in designated areas unless otherwise informed, e.g. for specific events and activities. Under no circumstance should images be taken at any time on school premises or on off-site school events and activities of anyone other than their own child, unless there is a pre-specified permission from Steve Morley or the Safeguarding Team. When a parent/carer is on school premises their phone/s should be switched off and out of sight.

Pupils are allowed to bring personal mobile devices/phones to school but the devices should not be used, seen or heard by staff; they should not be used and should be kept in bags/coats at all times. Under no circumstance should pupils use their personal mobile devices/phones to take images of

- any other pupil unless they and their parents have given agreement in advance
- any member of staff

This is covered within the Behaviour for learning Policy and if the phone is seen, heard or used with school there will be a consequence applied.

Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

Personal mobiles must never be used to access school emails and data. The only exception would be where a closed, monitorable system has been set up by the school for use on a personal device.

The school is not responsible for the loss, damage or theft of any personal mobile device that is brought into school.

New technological devices

New personal technological devices may offer opportunities for teaching and learning. However, the school will consider educational benefit and carry out risk assessment before use in school is allowed. Parents/carers, pupils and staff should not assume that new technological devices will be allowed in school and should check before they are brought into school.

Reporting incidents, abuse and inappropriate material

There may be occasions in school when either a pupil or an adult receives an offensive, abusive or inappropriate message or accidentally accesses upsetting or abusive material. When such a situation occurs the pupil or adult must report the incident immediately to the first available member of staff, the HOY/SSO, FT or SLT. Where such an incident may lead to significant harm, safeguarding procedures should be followed. The school takes the reporting of such incidents seriously and where judged necessary, the DSL will refer details to social care or the police.

5. Curriculum

Online safety is fully embedded within our curriculum. The school provides a comprehensive age appropriate curriculum for online safety which enables pupils to become informed, safe and responsible. This includes teaching to prevent radicalisation, for which staff provide a narrative to counter extremism. The RSE and IT curriculum are central in supporting the delivery of online safety education.

The curriculum is flexible and can respond to any immediate online safety issues and risks as they emerge.

It is necessary for pupils to develop skills of critical awareness, digital resilience and good online citizenship to enable them to use internet, mobile and digital technologies safely and responsibly. Pupils are taught to recognise the creative, collaborative, cultural, economic and educational opportunities provided by the internet, mobile and digital technologies. Curriculum work will also include areas such as:

- Understanding how to use the internet, mobile and digital technologies in a balanced and appropriate way to avoid negative impact on wellbeing, e.g. regulated screen time and diverse online activity
- Learning how to develop a positive online reputation and enhance future opportunities e.g. in relationships and employment
- Developing critical thinking skills and the confidence to challenge and question what they see and read in relation to online content e.g. recognising fake news and extremism, understanding commercial manipulation, maintaining an authentic sense of self that is resilient to online pressure, learning how easy it is to lie online (i.e. users may not be who they say they are and may have ulterior motives) Understanding the dangers of giving out personal details online and the importance of maintaining maximum privacy online
- Thinking carefully before placing images online and considering their appropriateness and understanding the importance of gaining consent before posting photographs of others

- Understanding the permanency of all online postings and conversations

Understanding relevant legislation, including copyright, and the importance of respecting other people's information, reputation and images.

- Understanding the importance of online respect and what constitutes cyberbullying, how to avoid it, the impact it has and how to access help.
- How the law can help protect against online risks and abuse.

6. Staff and Governor Training

Staff and governors are trained to fulfil their roles in online safety. The school audits the training needs of all school staff and provides regular training to improve their knowledge and expertise in the safe and appropriate use of internet, mobile and digital technologies. This training, if received, is recorded as part of staff CPD records.

New staff are provided with a digital copy of the online safety policy and must sign the school's Acceptable Use Agreement as part of their induction and before having contact with pupils.

Any organisation working with children and based on the school premises are also provided with a copy of the online safety policy and required to sign the Acceptable Use Agreement.

Peripatetic staff, student teachers and regular visitors are provided with a copy of the online safety policy and are required to sign the Acceptable Use Agreement.

Guidance is provided for occasional visitors, volunteers and parent/carers helpers who use the school ICT systems.

7. Working in Partnership with Parents/Carers

The school works closely with families to help ensure that children can use internet, mobile and digital technologies safely and responsibly both at home and school. The support of parents/carers is essential to implement the online safety policy effectively and help keep children safe.

It is important that parents/carers understand the crucial role they play in this process. The school seeks to regularly consult and discuss online safety with parents/carers and seeks to promote a wide understanding of the benefits of new technologies and associated risks. The school provides regular updated online safety information through the school website, newsletters and by other means.

8. Records, monitoring and review

The school recognises the need to record online safety incidents and to monitor and review policies and procedures regularly in order to ensure they are effective and that the risks to pupils and staff are minimised.

All breaches of this policy must be reported and all reported incidents will be logged. All staff have the individual responsibility to ensure that incidents have been correctly recorded, acted upon and reported. The Nobel School requires all staff to record all Online safety concerns on CPOMs.

The school supports pupils and staff who have been affected by a policy breach.

Where there is inappropriate or illegal use of internet, mobile and digital technologies, this will be dealt with under the school's behaviour and disciplinary policies as appropriate. Breaches may also lead to criminal or civil proceedings.

Governors receive termly summary data on recorded online safety incidents for monitoring purposes. In addition governors ensure they have sufficient, quality information to enable them to make a judgement about the fitness for purpose of this policy on an annual basis.

9. Appendices of the Online Safety Policy

- A. Guidance on the process for responding to cyberbullying incidents
- B. Guidance for staff on preventing and responding to negative comments on social media
- C. EXAMPLE: Online safety incident reporting form (**Please use CPOMs**)
- D. EXAMPLE: Online safety incident record (**Please use CPOMs**)
- E. EXAMPLE: Online safety incident log (**Please use CPOMs**)

Appendix A - Guidance on the process for responding to cyberbullying incidents

All cyberbullying incidents should be reported and responded to. Where the perpetrator is a member of the school community the majority of cases can be dealt with through mediation and/or disciplinary processes.

The following procedures are recommended:

- Never reply to the sender/poster of cyberbullying content. If applicable, block the sender.
- Incidents should be reported immediately. Pupils should report to a member of staff (e.g. class teacher, headteacher) and staff members should seek support from their line manager or a senior member of staff.
- The person reporting the cyberbullying should save the evidence and record the time and date. This evidence must not be forwarded but must be available to show at a meeting. Under no circumstances should indecent images of children and young people be printed or forwarded as this is a further criminal act. Staff should not ask to see the evidence of reported indecent images of children or young people but must refer this immediately to the police. Any member of staff being shown such evidence should immediately inform their line manager or the headteacher so that the circumstances can be recorded.
- A senior member of staff will meet with the person who has reported the incident and the target, if different, to listen, reassure and support. All relevant facts will be reviewed and documented.
- A senior member of staff will conduct an investigation.
- Anyone found to have cyberbullied will have attention drawn to the seriousness of their behaviour and if necessary the police will be involved. If the comments are threatening, abusive, sexist, of a sexual nature, constitute a hate crime or are libellous they may well break the law. Online harassment and stalking is also a crime.
- Once evidence has been secured then the person who has cyberbullied will be requested to remove the offending comments/material. Any refusal will lead to an escalation of sanctions.

Appendix B - Guidance for staff on preventing and responding to negative comments on social media

The school should make it clear which, if any, social media platforms are used to communicate with parents/carers. If used correctly, parents can use a school's social media site as a source of reliable information. The online safety policy, see especially Appendix F (Online safety policy guide - Summary of key parent/carer responsibilities), clarifies that no other social media platforms should be set up using the school's name or logo.

The school should regularly reinforce with all parties that discussion of school issues on social media platforms, either positive or negative, should not take place as this could bring the school into disrepute and affect families and children. Parents should be encouraged to be good online role models and not post statements written in anger or frustration. Identified routes to raise concerns directly with the school should be used.

If negative comments are posted:

- **Collect the facts**

As soon as you become aware of adverse comments relating to the school you need to establish what is being said. It is essential that if you have access to the postings they are secured and retained together with any other evidence. Do not become engaged in responding directly.

If the allegations against a member of staff or a pupil are of a serious nature, these will need to be formally investigated. This may involve the police and the headteacher will need to follow the school's safeguarding procedures.

If there is a risk of serious damage to the school reputation or the reputation of individual members of staff, professional legal advice should be sought.

Adverse comments of any kind are highly demotivating and cause stress and anxiety. It is important that the senior staff reassure and support all staff and/or other affected members of the school community.

- **Addressing negative comments and complaints**

Contact the complainants and invite them to a meeting. In the meeting, make sure you have any evidence available.

The meeting must:

- Draw attention to the seriousness and impact of the actions/postings;
- Ask for the offending remarks to be removed;
- Explore the complainant's grievance;
- Agree next steps;
- Clarify the correct complaints procedures.

If the meeting does not resolve the issue, the parents must be informed that the school will need to take the matter further. This may include:

- Reporting the matter to the social network site if it breaches their rules or breaks the law;
- Reporting the matter to the police if it breaks the law, e.g. if the comments are threatening, abusive, malicious, sexist, of a sexual nature, constitute a hate crime or are

libellous they may well break the law. Online harassment and stalking is also a crime.

If inappropriate postings continue or the original material is not removed, a second meeting is advisable to re-iterate the seriousness of the matter.

Appendix C - Online safety incident reporting form

Any member of the school community can raise a concern about an online safety incident. If you have witnessed or experienced an incident please complete the form below to help us to address the issue. It is important that you provide as much detail as possible. Once completed please hand this report to **XXXX**.

Name of person reporting incident:			
Signature:			
Date you are completing this form:			
Where did the incident take place:	Inside school?		Outside school?
Date of incident(s):			
Time of incident(s):			

Who was involved in the incident(s)?	Full names and/or contact details
Children/young people	
Staff member(s)	
Parent(s)/carer(s)	
Other, please specify	

Type of incident(s) (indicate as many as apply)			
Accessing age inappropriate websites, apps and social media		Accessing someone else's account without permission	
Forwarding/spreading chain messages or threatening material		Posting images without permission of all involved	
Online bullying or harassment (cyber bullying)		Posting material that will bring an individual or the school into disrepute	
Racist, sexist, homophobic, religious or other hate material		Online gambling	
Sexting/Child abuse images		Deliberately bypassing security	
Grooming		Hacking or spreading viruses	
Accessing, sharing or creating pornographic images and media		Accessing and/or sharing terrorist material	
Accessing, sharing or creating violent images and media		Drug/bomb making material	
Creating an account in someone else's name to bring them into disrepute		Breaching copyright regulations	
Other breach of acceptable use agreement, please specify			

Full description of the incident	What, when, where, how?
----------------------------------	-------------------------

Name all social media involved	Specify: Twitter, Facebook, Whatsapp, Snapchat, Instagram etc
Evidence of the incident	Specify any evidence available but do not attach.

Thank you for completing and submitting this form.

Appendix D - Online safety incident record

Name of person reporting incident:			
Date of report:			
Where did the incident take place:	Inside school?		Outside school?
Date of incident(s):			
Time of incident(s):			

Who was involved in the incident(s)?	Full names and/or contact details
Children/young person	
Staff member(s)	
Parent(s)/carer(s)	
Other, please specify	

Type of incident(s) (indicate as many as apply)			
Accessing age inappropriate websites, apps and social media		Accessing someone else's account without permission	
Forwarding/spreading chain messages or threatening material		Posting images without permission of all involved	
Online bullying or harassment (cyberbullying)		Posting material that will bring an individual or the school into disrepute	
Racist, sexist, homophobic, religious or other hate material		Online gambling	
Sexting/Child abuse images		Deliberately bypassing security	
Grooming		Hacking or spreading viruses	
Accessing, sharing or creating pornographic images and media		Accessing and/or sharing terrorist material	
Accessing, sharing or creating violent images and media		Drug/bomb making material	
Creating an account in someone else's name to bring them into disrepute		Breaching copyright regulations	
Other breach of Acceptable Use Agreement			
Other, please specify			

Full description of the incident	What, when, where, how?
----------------------------------	-------------------------

Name all social media involved	Specify: Twitter, Facebook, Whatsapp, Snapchat, Instagram etc
Evidence of the incident	Specify any evidence provided but do not attach

Immediate action taken following the reported incident:	
Incident reported to online safety Lead /DSP/ /Headteacher	
Safeguarding advice sought, please specify	
Referral made to HCC Safeguarding	
Incident reported to police and/or CEOP	
Online safety policy to be reviewed/amended	
Parent(s)/carer(s) informed please specify	
Incident reported to social networking site	
Other actions e.g. warnings, sanctions, debrief and support	
Response in the wider community e.g. letters, newsletter item, assembly, curriculum delivery	

Brief summary of incident, investigation and outcome (for monitoring purposes)	
---	--

Appendix E - Online safety incident log

Summary details of ALL online safety incidents will be recorded on this form by the online safety lead or other designated member of staff. This incident log will be monitored at least termly and information reported to SLT and governors.

Date & time	Name of pupil or staff member Indicate target (T) or offender (O)	Nature of incident(s)	Details of incident (including evidence)	Outcome including action taken