HIGH WELL SCHOOL
Preparing for Positive Futures

Online Safety

Policy Lead:	Adrian Coates
Date approved by Governing Body:	05.01.2023
Date Shared with Staff:	05.01.2023
Date of Review:	January 2024

Signed by Chair of Governors:	*Margaret Turner*
Date:	05.01.2023

Contents

1. Aims

This policy 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.

2. Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, 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 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 The Governing Body

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

The governing body will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the Designated Safeguarding Lead (DSL) and deputies.

All governors will:

- Ensure that they have read and understand this policy
- 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) Louise Quinn and the deputies are set out in our child protection and safeguarding policy.

Adrian Coates (Deputy Head teacher and Online Safety Lead) 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, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see appendix 4) 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
- Updating and delivering staff training on online safety, (appendix 3 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Headteacher and/or governing board
- This list is not intended to be exhaustive.

3.4 ICT support

We receive external ICT support on a weekly basis. The current provider is Alamo Business Systems. They are responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- 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 weekly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

This list is not intended to be exhaustive.

3.5 All staff and volunteers

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

- Maintaining an understanding of this policy
- Implementing this policy consistently
- 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 (appendix 1)
- Working with the Online Safety Lead to ensure that any online safety incidents are logged (see appendix 4) 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

This list is not intended to be exhaustive.

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 (appendix 1)

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

- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum.

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

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.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.

Online safety will also be covered during Pupil Progress Days. Parents will be provided with information on how their pupils have been educated in school and provided with advice on how to help keep their child safe at home.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headteacher and/or the Online Safety Lead.

Concerns or queries about this policy can be raised with any member of staff or the Headteacher.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps 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. Class teachers will discuss cyber-bullying with their tutor groups, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes PPF (Preparing for Positive futures) education, and other subjects where appropriate.

All staff receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 13 for more detail).

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 Headteacher will consider whether the incident should be reported to the police if it involves illegal material, and will 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, 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 Online Safety Lead 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.

7. Nudes and Semi Nudes

In the latest advice for schools and colleges (UKCIS, 2020), this is defined as the sending or posting of nude or semi-nude images, videos or live streams online by young people under the age of 18. This

could be via social media, gaming platforms, chat apps or forums. It could also involve sharing between devices via services like Apple's AirDrop which works offline.

Please report any instance to the Online Safety Lead or a Designated Safeguarding Lead (DSL)

- Never view, copy, print, share, store or save the imagery yourself, or ask a child to share or download – this is illegal.

- If you have already viewed the imagery by accident (e.g. if a young person has showed it to you before you could ask them not to), report this to the Online Safety Lead or DSL and seek support.

- Do not delete the imagery or ask the young person to delete it.

- Do not ask the child/children or young person(s) who are involved in the incident to disclose information regarding the imagery. This is the responsibility of the DSL.

- Do not share information about the incident with other members of staff, the young person(s) it involves or their, or other, parents and/or carers.

- Do not say or do anything to blame or shame any young people involved.

- Do explain to them that you need to report it and reassure them that they will receive support and help from the DSL.

8. Online Challenges and Hoaxes

Pupils will be provided with relevant education on online challenges and hoaxes within the ICT curriculum.

When we become aware of specific online challenges or hoaxes, we will take advice from the Local Authority safeguarding team. Generally speaking, naming an online hoax and providing direct warnings is not helpful. There have been examples of hoaxes where much of the content was created by those responding to the story being reported, needlessly increasing children and young people's exposure to distressing content. If we are confident children and young people are aware of, and engaged in, a real challenge that may be putting them at risk of harm, then it may be directly addressed, after consultation with the local authority.

If parents and carers have any concerns regarding Online Challenges please contact Mr Coates.

9. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but must put them into their locker on arrival. This includes all items which grant access to the internet including mobile phones, tablets, smart watches etc. Pupils will not have access to their device until the end of the school day.

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.

10. Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

11. Social Media

11.1 Expectations

- The expectations' regarding safe and responsible use of social media applies to all members of High Well School community.

- The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger.

- All members of High Well School community are expected to engage in social media in a positive, safe and responsible manner, at all times.

- All members of High Well School community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.

- The school will control pupil and staff access to social media whilst using school provided devices and systems on site.

- The use of social media during school hours for personal use is not permitted.

- Inappropriate or excessive use of social media during school/work hours or whilst using school devices may result in disciplinary or legal action and removal of internet facilities.

- Concerns regarding online conduct of any member of High Well School community on social media should be reported to the school and will be managed in accordance with our Disciplinary, Behaviour and Safeguarding & Child Protection Policies.

11.2 Staff Personal Use of Social Media

The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.

Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the school Code of conduct within the Staff Handbook.

11.3 Reputation

All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within school. Civil, legal or disciplinary action may be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

All members of staff are advised to safeguard themselves and their privacy when using social media sites. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include (but is not limited to):

- Setting the privacy levels of their personal sites as strictly as they can.

- Being aware of location sharing services.

- Opting out of public listings on social networking sites.

- Logging out of accounts after use.

- Keeping passwords safe and confidential.

- Ensuring staff do not represent their personal views as that of the school.

Members of staff are encouraged not to identify themselves as employees of High Well on their personal social networking accounts. This is to prevent information on these sites from being linked with the school and also to safeguard the privacy of staff members.

All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance with school's policies and the wider professional and legal framework.

Information and content that staff members have access to as part of their employment, including photos and personal information about pupils and their family members or colleagues will not be shared or discussed on social media sites.

Members of staff will notify the Leadership Team immediately if they consider that any content shared on social media sites conflicts with their role in the school.

11.4 Communicating with pupils and parents and carers

- All members of staff are advised not to communicate with or add as 'friends' any current or past pupils or current or past pupils' family members via any personal social media sites, applications or profiles.

- Any pre-existing relationships or exceptions that may compromise this will be discussed with the Online Safety Lead and/or the Headteacher.

- If ongoing contact with pupils is required once they have left the school roll, members of staff will be expected to use official school provided communication tools.

- Staff will not use personal social media accounts to make contact with pupils or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the Headteacher.

- Any communication from pupils and parents received on personal social media accounts will be reported to the schools Online Safety Lead.

12. Use of Personal Devices and Mobile Phones

High Well School recognises that personal communication through mobile technologies is an accepted part of everyday life for pupils, staff and parents/carers, but technologies need to be used safely and appropriately within school.

12.1 Expectations

- All use of personal devices and mobile phones will take place in accordance with the law and other appropriate school policies, including, but not limited to: Anti-bullying, Behaviour and Safeguarding and Child protection.

- Electronic devices of any kind that are brought onto site are the responsibility of the user at all times.

- All members of High Well School community are advised to take steps to protect their mobile phones or devices from loss, theft or damage; the school accepts no responsibility for the loss, theft or damage of such items on school premises.

- All members of the school community are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared.

- Mobile phones and personal devices are not permitted to be used in specific areas within the school site such as changing room and toilets

- The sending of abusive or inappropriate messages/ content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with as part of our Behaviour policy and staff code of conduct.

- All members of High Well School community are advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene the school Behaviour or Safeguarding and Child protection policies.

12.2 Staff Use of Personal Devices and Mobile Phones

Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as, relevant school policy and procedures, such as: Confidentiality, Safeguarding and Child protection, Data security and Acceptable use.

Staff will be advised to:

- Keep mobile phones and personal devices in a safe and secure place during lesson time

- Keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times.

- Ensure that Bluetooth or other forms of communication (such as 'airdrop') are hidden or disabled during lesson times.

- Not use personal devices during teaching periods, unless permission has been given by the Headteacher, such as in emergency circumstances.

- Ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations.

- Members of staff are not permitted to use their own personal phones or devices for contacting pupils or parents and carers.

- Any pre-existing relationships, which could undermine this, will be discussed with the Online Safety Lead and Headteacher.

Staff will not use personal devices, such as: mobile phones, tablets or cameras:

- To take photos or videos of pupils and will only use work-provided equipment for this purpose.

- To communicate directly with pupils, and will only use work-provided equipment during lessons/educational activities.

If a member of staff breaches the school policy, action will be taken in line with the school code of conduct and disciplinary policy

- If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence, the police will be contacted.

13. 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 the behaviour policy. 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 or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. 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.

14. 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 and staff meetings).

The DSL and deputies 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.

Volunteers will receive appropriate training and updates, if applicable.

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

15. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 4.

This policy will be reviewed annually by the SLT. At every review, the policy will be shared with the Governing Body.

16. Links with other policies

This online safety policy is linked to our:

Child protection and safeguarding policy, Behaviour Policy and Code of Conduct

Appendix 1: acceptable use agreement (pupils and parents/carers)

Acceptable use of the school's ICT systems and internet: agreement for pupils and parents/carers

Name of pupil:

When using the school's ICT systems and accessing the internet in school, I will not:

Use them for a non-educational purpose

Use them without a teacher being present, or without a teacher's permission

Access any inappropriate websites

Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity)

Use chat rooms

Open any attachments in emails, or follow any links in emails, without first checking with a teacher

Use any inappropriate language when communicating online, including in emails

Share my password with others or log in to the school's network using someone else's details

Give my personal information (including my name, address or telephone number) to anyone without the permission of my teacher or parent/carer

Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

If I bring a personal mobile phone or other personal electronic device into school:

I will put it into my locker as requested at the beginning of the school day and expect for it to be returned at the end of the school day.

I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

I agree that the school will monitor the websites I visit.

I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.

I will always use the school's ICT systems and internet responsibly.

Signed (pupil):	**Date:**

Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):	**Date:**

Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors)

Acceptable use of the school's ICT systems and the internet: agreement for staff, governors, volunteers and visitors

Name of staff member/governor/volunteer/visitor:

When using the school's ICT systems and accessing the internet in school:

- I will not browse, download or send material that could be considered offensive to colleagues. I will not access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature

- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may access

- I will not install/download any unauthorised software. I will not attempt to install or store software, or try to alter computer settings without permission and technical advice. I will ensure that USB devices containing data relating to the school are encrypted.

- I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too. I will not use them in a way that could harm the school's reputation.

- I will only use the approved, secure email system(s) for any school business. I will not use any improper language when communicating online, including in emails or other messaging services

- I will not access social networking sites or chat rooms. I will not publish anything on social media that could harm the school's reputation.

My use of the Internet, email and other related technologies can be monitored and logged by school where it believes unauthorised use of the schools information system may be taking place or the system may be being used for unauthorised or unlawful purposes.

I will not have my personal telephone during school hours unless I have permission from a member of SLT. I will not use mobile phones or the internet for personal use during working hours

I will let the Designated Safeguarding Lead (DSL) and Online Safety Lead (A Coates) 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 only use the approved school email/mobile to communicate with pupils or parents/carers, and only communicate with them on appropriate school business. I agree that I will not have any contact with pupils or parents via social media.

I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the DSL and Online Safety Lead (A Coates) who will log the incident and take appropriate action.

I will not connect a computer or laptop to the network / Internet that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the LA's anti-virus software.

Signed (staff member/governor/volunteer/visitor):	Date:

Appendix 3: online safety training needs – self-audit for staff

Online safety training needs audit	
Name of staff member/volunteer:	**Date:**
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training? Please record them here.	

Appendix 4: online safety incident report log

Online safety incident report log				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**