High Grange

Adaptive thinking, Communication, Emotional wellbeing, Independence

Promoting Wellbeing & Safety		
Cyberbullying		
Last Update: November **2025**	Responsible: **Principal**	Page: 1 of 11

This policy promotes ACE because;	
	**Adaptive thinking:** pupils use a simple Stop, Think, Check, Report routine to recognise risk, choose safe actions and seek help early. **Communication:** pupils and staff use respectful digital conduct, clear reporting routes to staff/the DSL and platforms, and gain consent before sharing images. **Emotional wellbeing & Independence:** pupils build resilience to cyberbullying and harmful content, set healthy screen-time boundaries, and know how to block, report and get support; they manage passwords and 2FA and understand digital footprints

Contents:

Statement of intent

High Grange School understands that everyone in the school community deserves to learn and teach in a supportive and caring environment, without fear of bullying or harassment.

Communication technology plays an increasingly large and important role in the school curriculum. As a result, it is important to acknowledge that, sometimes, new technologies can be used for unpleasant or illegal purposes.

We recognise the existence of cyberbullying and the severity of the issue.
The school is committed to:

- All types of bullying are handled as a community issue at High Grange School.
- Educating pupils, staff and parents about cyberbullying and its consequences.
- Providing a productive and healthy learning environment.
- Providing a robust policy in order to prevent and, if necessary, deal with any cyberbullying, should it arise at school or within the school community.
- Developing and improving the policies and procedures around cyberbullying through regular evaluation and review.
- Providing a strong anti-bullying policy and acting upon it wherever bullying arises.

1. Legal framework

- Equality Act 2010
- Education Act 2002
- Education and Inspections Act 2006 (discipline and behaviour powers)
- Education (Independent School Standards) Regulations 2014
- Protection from Harassment Act 1997
- Malicious Communications Act 1988
- Communications Act 2003, section 127
- Sexual Offences Act 2003 (indecent images of anyone under 18)
- Voyeurism (Offences) Act 2019
- Computer Misuse Act 1990 (as amended)
- Keeping children safe in education (KCSIE) 2025
- Preventing and tackling bullying (Department for Education, July 2017)
- Searching, screening and confiscation in schools (Department for Education, updated 19 July 2023)
- Behaviour in schools (Department for Education, 19 February 2024) Use of reasonable force in schools (Department for Education, updated 15 January 2025)
- Teaching online safety in schools (Department for Education, 12 January 2023)
- Mobile phones in schools (Department for Education, 19 February 2024)
- Working Together to Safeguard Children (December 2023)

This policy operates in conjunction with the following school policies:

- Acceptable Use Agreement
- E-safety Policy / Online safety
- Anti-bullying Policy
- Allegations of Abuse Against Staff Policy
- Child Protection and Safeguarding Policy
- Searching, Screening and Confiscation Policy
-

2. Roles and responsibilities

The board of directors / board of governance is responsible for:

- The overall implementation and monitoring of this policy.
- High Grange School Safeguarding link governor is Karen Noon who will work alongside the school to ensure the policies and practices relating to safeguarding,

including the prevention of cyberbullying, are being implemented effectively. Sue Wilkinson is the Finance governor / director who attends all leadership team meetings

The Principal is responsible for:

- The practices and procedures outlined in this policy and ensuring that their effectiveness is monitored.
- Ensuring that the school maintains details of agencies and resources that may assist in preventing and addressing cyberbullying.
- Reviewing the procedures outlined in the school's Online Safety to ensure that pupils protect themselves from cyberbullying online.
- Ensuring all incidents of cyberbullying are reported and dealt with in accordance with the school's Anti-Bullying Policy.

The DSL (SSL) is responsible for:

- Ensuring all policies that relate to safeguarding, including cyberbullying, are reviewed and updated regularly.
- Ensuring all staff are aware that they must report any issues concerning cyberbullying and know how to do so.
- Providing training to all staff so that they feel confident identifying pupils at risk of being cyberbullied and know how to make referrals when a pupil is at risk.
- Ensuring that parents are provided access to this policy so that they are fully aware of the school's responsibility to safeguard pupils and their welfare.
- Ensuring all pupils are taught about cyberbullying and how they should report a concern.
- Ensuring all staff are aware of their responsibilities by providing clear guidance for staff on the use of technology, both inside and outside of school.

All members of staff are responsible for identifying signs of cyberbullying and staying informed about the technologies that pupils commonly use.
Teachers are responsible for ensuring that issues surrounding cyberbullying are explored in the curriculum and pupils are aware of how to respect others.

Pupils, staff and parents are responsible for complying with the school's Acceptable Use Agreement.

Pupils will be asked to sign the agreement before they are allowed to use computer equipment and the internet in school. Parents will be asked to confirm that they have discussed its contents with their children.

3. What is cyberbullying?

For the purpose of this policy, "**bullying**" is an act which is based on unequal power relations, real or perceived. It will usually be repeated and be difficult to defend against and is intended to hurt the recipient emotionally and/or physically. It can manifest verbally, in writing or images, and can be done physically, financially (including damage

to property) or through social isolation. Verbal bullying is the most common form, especially within schools. (Refer to High Grange School's Anti Bulling Policy.

For the purpose of this policy, "**cyberbullying**" includes sending or posting harmful or upsetting text, images or other messages using the internet, mobile phones or other ICT for the purpose of bullying.

Cyberbullying can take many forms and can go even further than face-to-face bullying by invading personal space and home life, and can target more than one person. It can also take place across age groups and target pupils, staff and others, and may take place inside school, within the wider community, at home or when travelling. It can sometimes draw bystanders into being accessories.

Cyberbullying can include the following:

- Threatening, intimidating or upsetting text messages
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras
- Disclosure of private sexual photographs or videos with the intent to cause distress
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name
- Menacing or upsetting responses to someone in a chatroom
- Unpleasant messages sent via instant messaging
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook
  NB. The above list is not exhaustive, and cyberbullying may take other forms.

All cases of cyberbullying are considered to be as serious as any other form of bullying.

Cyberbullying issues are dealt with in an appropriate manner dependent on the severity and frequency of the issue, in accordance with the school's Anti-Bullying Policy

4. Legal issues

Cyberbullying is generally criminal in character. It is unlawful to disseminate defamatory information in any media, including via websites. Section 127 of the Communications Act 2003 makes it an offence to send, by public means of a public electronic communications network, a message or other matter that is grossly offensive, or one of an indecent, obscene or menacing character. In addition, the Protection from Harassment Act 1997 makes it an offence to knowingly pursue any course of conduct amounting to harassment. At the school, cyberbullying is considered as serious as any other form of bullying. Cyberbullying issues are dealt with in an appropriate manner dependent on the severity and frequency of the issue and the age of the pupil.

5. Preventing cyberbullying

The school recognises that both staff and pupils may experience cyberbullying and will commit to preventing any instances that may occur by creating a learning and teaching environment which is free from harassment and bullying.

Our curriculum is mapped to Teaching online safety in schools (2023) and the UKCIS Education for a Connected World framework. The school's approach to mobile phones follows DfE Mobile phones in schools (2024) and the Behaviour Policy; breaches attract proportionate sanctions.

Staff, pupils and parents will be regularly educated about cyberbullying and the importance of staying safe online, in accordance with the school's Online Safety Policy Teachers will discuss cyberbullying as part of the curriculum, and diversity, difference and respect for others will be promoted and celebrated through various lessons. This is particularly targeted in PSHE and Computing across all key stages.

Pupils will be educated about the importance of reporting instances of cyberbullying and will be fully informed of who they should report any concerns to.

The school will provide opportunities to extend friendship groups, and interactive skills will be provided through participation in special events. High Grange School has whole school calendar events across the school year including;

- Winter Showcase (Autumn 2 term)
- Spring Talent Show (Spring 2 term)
- Summer Fayre (Summer 2 term)
- World Book Day
- Sports Day
- Red Nose Day
- Sport Relief Mile
- Sports Fixtures
- House events (between 10-12 every term)

Staff will be regularly educated about the signs of cyberbullying in order to promote early identification and intervention. High Grange School ensure annual training from external Online Safety expert Traci Good. High Grange School CEOP ambassador Nathan Barrington – provides annual internal training at least annually. Alison Seager Spicer is the school's pastoral teacher and mental health first aider. Alison Seager Spicer is a trained crisis counsellor – she is also trained NSPCC crisis counsellor (Volunteer) – she will offer support and advice to pupils who encounter cyberbullying. Alison Seager Spicer will also support pupils who have cyberbullied another peer in school or out of school. All staff are trained in restorative justice. The school promotes a restorative approach to all types of Bullying including Cyberbullying.

Pupils will know how to report cyberbullying and they know who the safeguarding leads are in school to help keep them safe online. It is made clear in staff meetings and the staff code of conduct that members of staff should not have contact with current pupils on social networking sites (specifically, not befriending pupils on Facebook). In addition, staff are discouraged from having past pupils as friends.

The delivery of PSHE is important and will include discussing keeping personal information safe and the appropriate use of the internet. In addition, pupils will be educated about online safety with a clear focus upon 'trolling' / internet Trolls. High Grange School Computer Curriculum also educates pupils across all aspects of online safety and cyberbullying.

Outside the curriculum, pupils will receive regular pastoral sessions about online safety and cyberbullying through enrichment mornings / afternoons and drop down days. High Grange School has set calendar targeted and focused days / weeks such Anti-Bullying Week, Children's mental Health Week and Young Minds week.

Pupils will have a voice through the student council to ensure they are fully engaged and involved in evaluating and improving the school offer, school events and school improvement from a pupil perspective.

6. Signs of being cyberbullied

All members of staff will receive training on an annual basis on the signs of cyberbullying / online safety, in order to identify pupils who may be experiencing issues and intervene effectively.

Staff will be alert to the following signs that may indicate a pupil is being cyberbullied:

- Becoming withdrawn or shy
- Showing signs of depression
- Becoming extremely moody or agitated
- Becoming anxious or overly stressed
- Displaying signs of aggressive behaviour
- Avoiding use of the computer
- Changing eating and/or sleeping habits
- Avoiding participating in activities they once enjoyed
- Engaging in self-harm, or threatening/attempting suicide
- Changing their group of friends suddenly

Staff will also be alert to the following signs which may indicate that a pupil is cyberbullying others:

- Avoiding using the computer or turning off the screen when someone is near
- Appearing nervous when using the computer or mobile phone
- Acting in a secretive manner when using the computer or mobile phone
- Spending excessive amounts of time on the computer or mobile phone
- Becoming upset or angry when the computer or mobile phone is taken away

Parents will also be invited to attend online training sessions by Traci Good in order to educate them on the signs and symptoms of online safety. Parents have direct contact through the school's parent liaison officer and they can report any bullying or cyberbullying. High Grange School support parents through the school's website and through termly parent newsletter where there is a different 'parent corner' article every term. Parents will be advised to report to the Principal if their child displays any of the signs associated with cyberbullying.

7. Procedures for dealing with cyberbullying

All cyberbullying concerns are safeguarding matters. Staff must inform the DSL the same day, record on SchoolPod, and follow safeguarding procedures alongside this policy. Keep evidence (screenshots, URLs, message logs) where safe to do so; do not view suspected nudes/semi-nudes.

All issues of cyberbullying should be reported according to the procedures outlined in the Anti-Bullying Policy.

If staff are concerned that a pupil might be at risk of cyberbullying, they will report this to the schools safeguarding leads as soon as possible.

All pupils will be informed that they can disclose cyberbullying concerns about themselves or others to any member of staff. Staff will not promise confidentiality and will inform the DSL (SSL) of the disclosure as soon as possible.

Responses to cyberbullying incidents, including the necessary sanctions, will be dealt with in accordance with the school's Anti-Bullying Policy and the school promoting Good Behaviour and Discipline Policy

A cyberbullying incident might include features different to other forms of bullying, prompting a particular response. Significant differences may include the following:

- **Impact**: possible extensive scale and scope
- **Location**: the anytime and anywhere nature of cyberbullying
- **Anonymity**: the person being bullied might not know who the perpetrator is
- **Motivation**: the perpetrator might not realise that their actions are bullying
- **Evidence**: the subject of the bullying may have evidence of what has happened

Any cyberbullying incidents that involve members of staff will be dealt with in accordance with High Grange School's Anti-Bullying Policy and Staff and Allegations Against Staff Policy / HGS disciplinary policies and procedures.

Staff are required to report any concerns to the Principal, who will investigate the matter and will initiate an appropriate response.

All incidents of cyberbullying, including any concerns, will be recorded and securely held by the school's senior leadership team. This will be recorded on Behaviour watch and actions taken recorded.

High Grange Schools Pastoral Teacher or Clinical Psychologist will arrange a discussion with the victimised pupil in order to gain knowledge about the situation, and will use this to inform a discussion with the pupil who has been accused of cyberbullying. High Grange School will use where possible restorative approaches to support both the victim and the perpetrator. If the perpetrator keeps cyberbullying the same pupil or different pupil's, then the Schools Senior Leadership Team will look at escalating their response and invite parents into school to discuss the matter. If a resolution is still not achieved,

then the School's Principal will look at fix term exclusion and in extreme circumstances permanent exclusion. High Grange School has a zero tolerance of any type of bullying either in school and positively attempts to impact on bullying that occurs outside of school.

The Principal will discuss the incident with any witnesses and will gain evidence of the cyberbullying incident; this may involve text messages, emails, photos, etc., provided by the victim.

High Grange School has a primary setting. The school understands that pupils at primary level, and particularly younger children, may not be aware of their actions and, as such, may not mean to intentionally cyberbully another pupil.

The Principal will take into account the nature of the cyberbullying incident and the way in which it has been conducted, including if it is evident that it was intentional or if the pupil's age and knowledge of cyberbullying is a contributing factor to the incident, when deciding on the appropriate sanction. It is the school's intention to always show the pupil 'a better way' and obtain a 'positive learning outcome.'

If necessary, the Principal may decide to involve the police in an appropriate response to the cyberbullying incident.

If necessary, the Principal will liaise with the other members of the senior leadership team, safeguarding officers, the CEOP ambassador when issuing an appropriate sanction, such as by removing internet access by removing their login accounts, removing the pupils access to computers / phones in school, monitoring the pupil's internet use in, have 1-1 staffing ratio when accessing school technology devices. This will be in accordance with the online safety policy.

8. Support for the pupil being bullied

The Principal will discuss the support available with the victim and, therefore, their feelings and requests are paramount to the support provided.
The support available includes:

- Emotional support and reassurance from the schools Pastoral Teacher / Clinical Psychologist / CEOP ambassador. This may also include further support from the pupil's form staff, their keyworker and the schools Senior Leadership Team.
- Reassurance that it was right to report the incident and that appropriate action will be taken.
- Liaison with the pupil's parents to ensure a continuous dialogue of support.
- Advice not to retaliate or reply, but to keep the evidence and show or give it to their parent or a member of staff.
- Advice on other aspects of online safety procedures to prevent re-occurrence.
- Discussion with the pupil's parents to evaluate their online culture.
- Age-appropriate advice on how the perpetrator might be blocked online.
- Actions, where possible and appropriate, to have offending material removed.

- Discussion with the pupil's parents on whether police action is required (except in serious cases of child exploitation where the police may be contacted without discussion with parents).

The school will also use additional support, such as involvement with external agencies, where necessary, as outlined in the Anti-Bullying Policy.

9. Investigation and legal powers

The nature of any investigation will depend on the circumstances. It may include the following:

- Preserving evidence, for example, by saving or printing (e.g. phone messages, texts, emails and website pages)
- Efforts to identify the perpetrator, which may include looking at the media, systems and sites used. Staff may search a device and examine data where there is good reason to suspect it has been, or could be, used to cause harm, disrupt teaching or break school rules, in line with DfE "Searching, screening and confiscation". Any access to data, retention or deletion must be necessary and proportionate, recorded in the search log, and the DSL informed. Staff must not view/delete nudes or semi-nudes; the DSL leads the response using UKCIS guidance.
- Identifying and questioning witnesses
- Contacting the CEOP centre if images might be illegal or raise child protection issues
- Requesting that a pupil reveals a message or other phone content or confiscating a phone
- Legal action, e.g. where private sexual videos or images of an individual under 16-years-old are disclosed with the intent to cause distress

10 Working with the perpetrator

How the school will work with the perpetrator and any sanctions given will be determined on an individual basis in accordance with the Anti-Bullying Policy with the intention of:

- Helping the victim to feel safe again and be assured that the bullying will stop.
- Holding the perpetrator to account, so they recognise the harm caused and do not repeat the behaviour.
- Helping bullies to recognise the consequences of their actions and facilitating change in their attitude and behaviour.
- Demonstrating that cyberbullying, as with any other form of bullying, is unacceptable, and that the school has effective ways of dealing with it.

11 Staff Advice and Support

All school staff are in a position of trust, and there are expectations that they will act in a professional manner at all times. Here is some key advice for staff which may help protect their online reputation

- Ensure you understand your school's policies on the use of social media
- Child net's 'Using Technology' guide has more information on what to be aware of.

- Do not leave a computer or any other device logged in when you are away from your desk.
- Enabling a PIN or passcode is an important step to protect you from losing personal data and images (or having them copied and shared) from your mobile phone or device if it is lost, stolen, or accessed by pupils.2
- Familiarise yourself with the privacy and security settings of the social media and apps you use and ensure they are kept up to date. Advice can be found on the Safer internet advice and resources for parents and carers. On school site advice can be sought from Nathan Satterthwaite, Nathan Barrington and Daniel Hunnisett.
- It is a good idea to keep a check on your online presence – for example by typing your name into a search engine.
- If there is negative content on-line it is much easier to deal with this as soon as it appears. The UK Safer Internet Centres Reputation mini site has more information on this.
- Be aware that your reputation could be harmed by what others share about you online, such as friends tagging you in inappropriate posts, photographs, or videos.
- Consider your own conduct online; certain behaviour could breach your employment code of conduct.
- Discuss these same issues with close family, friends and colleagues, as you could become a target if they do not have security and privacy settings in place.
- Do not accept friend requests from pupils past or present. If you feel this is necessary, you should first seek guidance from a senior manager. Be aware that your social media friends may also be friends with pupils and their family members and therefore could read your post if you do not have appropriate privacy settings.
- Do not give out personal contact details – if pupils need to contact you with regard to homework or exams, always use your school's contact details.
- Use your school email address for school business and personal email address for your private life; do not mix the two. This includes file sharing sites; for example, Dropbox and YouTube.

12. Conclusion

This policy will be reviewed on an annual basis by the Principal who will make any changes necessary, taking into account previous cyberbullying incidents and the effectiveness of procedures, and will communicate changes to all members of staff.

All members of staff are required to familiarise themselves with this policy as part of their training programme.

This policy is reviewed annually (or sooner if guidance changes). Incident data and trends are reviewed termly by the DSL and SLT and reported to governors.