



Highclare School

Online Safety Policy

This policy applies to all sections of the school including EYFS, TOPS, PREP (Homework Club) and Holiday Care groups and is available to all parents and prospective parents on the website and from the school office on request.

Introduction

Following Government guidance, this policy has been agreed by senior management and approved by the school governing body.

Aims

The Internet is an essential element in education, business and social interaction. We, as a school, aim to provide pupils with quality internet access as part of their learning experience.

This policy is consistent with our three school aims.

The school will ensure that:

- Pupils and their parents are provided with a copy of the Acceptable Use Policy for ICT (see Appendix 1) when the pupil joins the school. This is printed in pupil planners
- Pupils are regularly reminded of on-line safety rules.
- The ICT programs of study teach on-line safety skills.
- Teachers in all curriculum areas using ICT to enhance teaching and learning are aware of, and teach about, Internet safety.
- Pupils in Key stages 1, 2, 3, 4 and 5 are aware of, and comply with, relevant legislation when using the Internet, including:
 - General Data Protection Regulation (GDPR).
 - Computer misuse.
 - Copyright and intellectual property legislation.
- Pupils are clear about where to seek help and advice, should they experience any problems when using the Internet.
- Staff, pupils and parents are aware that the school utilises surveillance software which records any detected instances of inappropriate use of the Internet. This software also restricts Internet access by filtering. However, the growth of websites makes it impossible to guarantee that all offensive or dangerous materials will always be covered.
- A monitoring and filtering software program, Smoothwall has been installed and immediately alerts the DSL and senior leaders if a pupil or member of staff types anything inappropriate into a search engine.
- Staff, pupils and parents are clear that the introduction of violent, degrading or sexual electronic materials into the school will not be tolerated.
- Education and information is provided to help build resilience in the pupils so that they may better protect themselves and their peers.
- Staff are trained in online safety as part of their safeguarding professional learning and development.
- Regular online safety workshops take place for parents

Actions the school is taking to ensure online safety.

1 Teaching online safety

- School ICT lessons will cover internet technologies and will teach online safety throughout.
- Pupils will be taught what internet use is acceptable, and what is not, and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- The school internet access will be designed expressly for pupil use and will include filtering appropriate to the age of the pupils.
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

- Pupils will be taught about positive uses of AI and how to critically evaluate responses given by AI

2 Communicating online safety

- Staff and pupils will be informed that Internet use will be monitored.
- Online safety rules will be communicated to pupils and parents at the beginning of the year.
- Online safety rules will be discussed with pupils at every possible opportunity.
- All staff will be given the online safety policy and its importance will be explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is therefore essential at all times.
- The ICT Acceptable Use Agreement for pupils is printed in student planners and signed annually by both parents and pupils
- Parents' attention will be drawn to the online safety Policy in newsletters, via the school parent portal and during online safety day/week.
- Prep School host parental workshops and drop in sessions throughout the year on online safety.

3 Monitoring Internet Activity

Internet sites

- The ICT team has a web surveillance facility available to them which incorporates web monitoring and filtering.
- The ICT department, with help and advice from the Senior Leadership Team, will ensure that the filtering methods selected are appropriate, effective and reasonable.
- If staff or pupils discover an unsuitable site, it must be reported to the ICT department by email to ictsupport@highclareschool.co.uk as soon as possible.
- In order to ensure that pupils are safe from terrorist and extremist material when accessing the internet in school, the ICT department will ensure that appropriate levels of filtering are in place in accordance with 'Prevent' duty guidance.

Social Networking Sites

- The school will block all access to social networking sites and instant messaging sites for all pupils and most staff. Designated members of staff using school Facebook, Instagram and Twitter (X) accounts will be granted access with agreement from the Head.
- Pupils will be advised never to give out personal details of any kind and should only consider real people that they know, to be their friends online.
- Staff, pupils and parents will be advised to be very careful when using social networking sites outside of school. We draw attention to the following:
 - Anything placed onto the Internet is effectively put into the public domain.
 - Whilst membership of sites can be restricted, it is not possible to control the way that other people use material that one gives access to.
 - Inappropriate comments about other staff or pupils made on a social network, instant message site or by email are always unacceptable.
Staff should not add pupils to their social networking sites other than to systems set up by the school for teaching and learning that should have built in user identification and archiving tools. The school has a virtual learning environment (VLE) which should be used for networking in the school community.
 - Staff should also refrain from adding recent former pupils to their social networking sites as they may provide an indirect link to current pupils. In line with the safe working practices for all staff contained within the Safeguarding Policy and Procedures.
 - Staff should also refrain from adding current parents to their social networking sites as they may provide an indirect link to current pupils. The School has a Facebook, Instagram and Twitter (X) account and communication should be via these sites only or the School VLE.
 - Staff should always be aware of the importance of confidentiality.

E-mail

- All emails sent with a Highclare School email address will reflect upon the school and should be carefully reviewed before sending, and given the same attention as a letter written on school headed paper.

- Materials that could be deemed offensive in any way should not be sent from a school email address.
- Staff and pupils may not use their personal email on the school network and access to these is blocked.
- Pupils must immediately tell a teacher if they receive offensive emails at school.
- Pupils must not reveal personal details of themselves or others in e-mail communication.
- The forwarding of chain letters is not permitted whilst using email on the school network.
- Pupils are provided with a school email address on admittance to the school which is to be used for school business. Any inappropriate use should be reported.

Highclare Virtual

- The name used for the school VLE is Highclare Virtual
- Highclare Virtual is to be the main means of communication for school related business.
- Highclare Virtual is the most effective way of communication between staff, pupils and parents. Staff and parents have been trained in its use.
- Pupils and staff will be advised about acceptable conduct and use when using Highclare Virtual.
- Only members of the current pupil, parent/carers and staff community will have access to Highclare Virtual.
- All users will be mindful of copyright issues and will only upload appropriate content onto Highclare Virtual.
- When staff, pupils etc leave the school their account or rights to specific school areas will be disabled.
- There is an online safety section on Highclare Virtual that informs pupils and their families of simple steps they can take to ensure online safety.

Firewall and Anti-Virus

- The school has a 24/7/365 Antivirus software that is updated on a continuous basis.

4 The School website and other external media

- The School makes various uses of images of pupils during their time at School. One use is to market the school in some external media. Media used, including photos of pupils at work or playing games, may include, but not limited to, the following
 - School website
 - Weekly digital news bulletin
 - School's Facebook, Instagram and Twitter (X)
 - School Prospectus
 - Items in the local press

Media usage is always carried out on the basis of parental consent (which can be withdrawn at any time) and, for members of U4 (Yr9) or above in the Senior School, pupil's own consent for a specific use.
- The contact details on the website will be the school address, email and telephone number. Staff or pupils' personal information will not be published.

5 Managing Emerging Technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out prior to the school permitting their use.

6 Online safety Complaints

Staff, pupils and parents will be informed of the procedure to follow in the event of an inappropriate incident.

Pupils

- A senior member of staff will deal with complaints of Internet misuse.
- Issues of a child protection nature must be dealt with in accordance with school child protection procedures and police will be contacted if appropriate.
- All concerns are recorded using CPOMS

Staff

- Any issues regarding staff misuse must be referred to the Head.

7 Failure to comply

Minor offences

Normal school procedures will be followed and relevant sanctions imposed. Alleged perpetrators will be dealt with fairly. Some pupils may not at first realise the seriousness of their actions such as passing on a copy of an offensive message to a friend. It must be made clear to the alleged offender that anyone who participates in the distribution of offensive material is supporting and reinforcing unacceptable use and behaviour.

Serious offences

In the opinion of the school the following breaches of the online safety Policy and / or Acceptable Use Policy constitute serious offences:

- Bullying / harassment or racism
- Serious breach of a person's privacy (hacking of restricted network drives – use of video on mobile devices to cause embarrassment or offence)
- Deliberate introduction of viruses into the school
- Deliberately accessing, downloading or disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent.
- Use of school's ICT infrastructure to procure illegal (or age limited) substances e.g. alcohol, drugs etc.
- Possession of illegal images.
- Misuse of technology to create and upload inappropriate material
- Use of the school's infrastructure for any form of gambling

The discovery or reporting of a serious offence such as those described above will require immediate investigation by the ICT Dept and senior members of staff. Where appropriate, the immediate involvement of the school's Designated Safeguarding Lead (DSL) will be sought.

For cases where pornography of minors, aggravated bullying, or the use of controlled substances is indicated the immediate involvement of the Police will be required.

Any breaches of the online safety policy will be dealt with under the school's Behaviour Policy and, in serious breaches, are likely to result in suspension or exclusion.

8. Cyberbullying

Procedures to follow:

- Make sure the pupil knows not to retaliate or return the message
- Ask the pupil to think about what information they have in the public domain
- Help the pupil to keep relevant evidence for any investigation (e.g. by not deleting messages they've received, and by taking screen capture shots and noting web addresses of online cyberbullying instances)
- Check the pupil understands simple ways to prevent it from happening again, e.g. by changing contact details, blocking contacts or leaving a chatroom

Action to contain the incident when content has been circulated:

- If you know who the person responsible is, ask them to remove the content
- Contact the host (eg the social networking site) to make a report to get the content taken down
- Ask the pupil to tell you who they have sent messages on to
- In cases of illegal content, consider contacting the police, who can determine what needs to be kept for evidential purposes.
- In cases of child protection, particularly in relation to incidences of child-on-child abuse (in line with Part 5 of Keeping Children Safe in Education 2026) the School is aware that information sharing should take place where necessary, regardless of what level of involvement there is from other agencies and that the GDPR and Data Protection Act 2018 do not prevent the sharing of information in such circumstances.

Related Policies:	• Anti-Bullying Policy	• ICT Agreements	• Safeguarding Policy
	• Behaviour Policy	• Mobile Device Policy	(Addendum refers to online safety during remote learning)
	• Code of Conduct (Staff)	• Privacy Notice – General	
	• Employee Handbook	• Privacy Notice – Pupil	

Adopted by the Board:	Review Cycle	Most Recent Review
September 2013	Annual	September 2026

Appendices:

- Acceptable use agreements (staff and pupils)