



HORRIS HILL

FOUNDED 1888

Online Safety Policy

Policy reviewed:	Autumn term 2021
Policy approval:	Reviewed by SJB Autumn 2021 Approved by Forfar Education Autumn 2021
Date of next review:	Autumn 2022

Online Safety Policy

1 Scope

- 1.1 The School is committed to promoting and safeguarding the welfare of all pupils and an effective online safety strategy is paramount to this. This Policy should be read in conjunction with relevant sections of the Safeguarding and Child Protection Policy and Procedures. The school fulfils the requirements of having an appropriate policy.
- 1.2 The aims of the School's online safety strategy are threefold:
 - 1.2.1 To protect the whole School community from illegal, inappropriate and harmful content or contact;
 - 1.2.2 To educate the whole School community about their access to and use of technology; and
 - 1.2.3 To establish effective mechanisms to identify, intervene and escalate incidents where appropriate.
- 1.3 In considering the scope of the School's online safety strategy, the School will take a wide ~~and purposive~~ approach to considering what falls within the meaning of technology, networks and devices used for viewing or exchanging information including communications technology (collectively referred to in this policy as **Technology**).
- 1.4 This policy applies to all members of the School community, including staff and volunteers, pupils, parents and visitors, who have access to the School's Technology whether on or off School premises, or otherwise use Technology devices in a way which affects the welfare of other pupils or any member of the School community or where the culture or reputation of the School are put at risk.
- 1.5 The following policies, procedures and resource materials are also relevant to the School's online safety practices:
 - 1.5.1 Acceptable Use Policy for Pupils
 - 1.5.2 Staff IT Acceptable Use Policy and Social Media Policy
 - 1.5.3 Safeguarding and Child Protection Policy and Procedures
 - 1.5.4 Peer on Peer Abuse Policy
 - 1.5.5 Bullying Policy: Preventing and Tackling
 - 1.5.6 Risk Assessment Policy for Pupil Welfare
 - 1.5.7 Staff Code of Conduct
 - 1.5.8 Data Protection Policy for Staff
- 1.6 These policies procedures and resource materials are available to staff on the staff area of the network and hard copies are available, either in the Staff Common Room or on request from the Bursary.
- 1.7 This is a whole school policy.

2 Roles and responsibilities

2.1 The Proprietor, Forfar Education

- 2.1.1 The Proprietor has overall responsibility for safeguarding arrangements within the School, including the School's approach to online safety and the use of Technology within the School.
- 2.1.2 The Proprietor is required to ensure that all those with leadership and management responsibilities at the School actively promote the well-being of pupils. The adoption of this policy is part of the Governing Body's response to this duty.
- 2.1.3 The Proprietor's Board Level Lead for Safeguarding is the senior board level lead with leadership responsibility for the School's safeguarding arrangements, including the School's online safety procedures, on behalf of the Proprietor.
- 2.1.4 The Proprietor will undertake an annual review of the School's safeguarding procedures and their implementation, which will include consideration of the effectiveness of this policy and related policies in meeting the aims set out in paragraph 1.2 above.

2.2 Headmaster and Senior Management Team

- 2.2.1 The Headmaster has overall executive responsibility for the safety and welfare of members of the School community.
- 2.2.2 The Designated Safeguarding Lead is the senior member of staff from the School's management team with lead responsibility for safeguarding and child protection, including online safety. The responsibility of the Designated Safeguarding Lead includes managing safeguarding incidents involving the use of Technology in the same way as other safeguarding matters, in accordance with the School's Safeguarding and Child Protection Policy and Procedures.
- 2.2.3 The Designated Safeguarding Lead will work with the Bursar, Head of Pastoral, Deputy Headmasters and the school's IT provider (see below) in monitoring Technology uses and practices across the School and assessing whether any improvements can be made to ensure the online safety and well-being of pupils.
- 2.2.4 The Designated Safeguarding Lead will regularly monitor and consider any alerts generated by software packages used to monitor and restrict use of the School's IT systems.
- 2.2.5 The Designated Safeguarding Lead will regularly update other members of the School's Senior Management Team on the operation of the School's safeguarding arrangements, including online safety practices.

2.3 Bursar and Designated Safeguarding Lead (DSL)

- 2.3.1 The Bursar, together with the Designated Safeguarding Lead and the school's IT provider, is responsible for the effective operation of the School's filtering system so that pupils and staff are unable to access any material that poses a safeguarding risk, including terrorist and extremist material, while using the School's network.

2.3.2 The Bursar is responsible for ensuring that:

- (a) the School's Technology infrastructure is secure and, so far as is possible, is not open to misuse or malicious attack;
- (b) the user may only use the School's Technology if they are properly authenticated and authorised;
- (c) the School has an effective filtering policy in place and that it is applied and updated on a regular basis;
- (d) the risks of pupils and staff circumventing the safeguards put in place by the School are minimised;
- (e) the use of the School's Technology is regularly monitored to ensure compliance with this policy and that any misuse or attempted misuse can be identified and reported to the appropriate person for investigation; and
- (f) monitoring software and systems are kept up to date to allow the ICT team to monitor the use of email and the internet over the School's network and maintain logs of such usage.

2.3.3 The school will constantly monitor internet use and review our filtering processes for any breaches through the use of Lightspeed and Impero software.

2.3.4 The DSL will report regularly to the Senior Management Team on the operation of the School's Technology. If the DSL has concerns about the functionality, effectiveness, suitability or use of Technology within the School, he will escalate those concerns promptly to the appropriate members(s) of the School's Senior Management Team.

2.3.5 The DSL is responsible for logging technology incidents on Engage and bringing any matters of safeguarding concern to the attention of the Headmaster in accordance with the School's Safeguarding and Child Protection Policy and Procedures.

2.4 **All staff**

2.4.1 The School staff have a responsibility to act as a good role model in their use of Technology and to share their knowledge of the School's policies and of safe practice with the pupils.

2.4.2 Staff are expected to adhere, so far as applicable, to each of the policies referenced in paragraph 1.5 above.

2.4.3 Staff have a responsibility to report any concerns about a pupil's welfare and safety in accordance with this policy and the School's Safeguarding and Child Protection Policy and Procedures.

2.5 **Parents**

2.5.1 The role of parents in ensuring that pupils understand how to stay safe when using Technology is crucial. The School expects parents to promote safe practice when using Technology and to:

- (a) support the School in the implementation of this policy and report any concerns in line with the School's policies and procedures;

- (b) talk to their child to understand the ways in which they are using the internet, social media and their mobile devices and promote responsible behaviour; and
- (c) encourage their child to speak to someone if they are being bullied or otherwise are concerned about their own safety or that of another pupil or need support.

2.5.2 If parents have any concerns or require any information about online safety, they should contact the Designated Safeguarding Lead.

3 Education and training

3.1 Pupils

3.1.1 The safe use of Technology is integral to the School's ICT curriculum. Pupils are educated in an age appropriate manner about the importance of safe and responsible use of Technology, including the internet, social media and mobile electronic devices (see the School's Curriculum Policy).

3.1.2 The safe use of Technology is also a focus in all areas of the curriculum and key safety messages are reinforced as part of assemblies and tutorial / pastoral activities, teaching pupils:

- (a) about the risks associated with using the Technology and how to protect themselves and their peers from potential risks;
- (b) to be critically aware of content they access online and guided to validate accuracy of information;
- (c) how to recognise suspicious, bullying or extremist behaviour;
- (d) the definition of cyberbullying, its effects on the victim and how to treat each other's online identities with respect;
- (e) the consequences of negative online behaviour; and
- (f) how to report cyberbullying and / or incidents that make pupils feel uncomfortable or under threat and how the School will deal with those who behave badly.

3.1.3 The School's Acceptable Use Policy for Pupils sets out the School rules about the use of Technology including internet, email, social media and mobile electronic devices, helping pupils to protect themselves and others when using Technology. Pupils are reminded of the importance of this policy on a regular basis.

3.2 Staff

3.2.1 The School provides training on the safe use of Technology to staff so that they are aware of how to protect pupils and themselves from the risks of using Technology and to deal appropriately with incidents involving the use of Technology when they occur.

3.2.2 Induction training for new staff includes training on the School's online safety strategy including this policy, the Staff Code of Conduct, Staff IT Acceptable Use Policy and Social Media Policy. Ongoing staff development training includes

training on Technology safety together with specific safeguarding issues including cyberbullying and radicalisation.

3.2.3 Staff also receive data protection training on induction and at regular intervals afterwards.

3.2.4 The frequency, level and focus of all such training will depend on individual roles and requirements and will be provided as part of the School's overarching approach to safeguarding.

3.3 Parents

3.3.1 The school will seek to provide information and awareness to parents through:

Acceptable use agreements for children
Curriculum activities involving raising awareness around staying safe online
Information included in briefing letters and newsletters
Parents evenings / sessions
High profile events / campaigns e.g. Safer Internet Day
Building awareness around information that is held on relevant web sites and or publications
Online Safety Policy

3.3.2 Parents are encouraged to read the Acceptable Use Policy for Pupils with their son to ensure that it is fully understood.

3.4 Useful resources

3.4.1 The Designated Safeguarding Lead will ensure that useful resources are made available to staff with regard to the safe use of Technology.

4 Access to the School's Technology

4.1 The School provides internet access and an email system to pupils and staff as well as other Technology. Such access is controlled by software permissions agreed by the Bursar and the Head of Pastoral with the school's IT provider and implemented by the school's IT provider. Pupils and staff must comply with the respective Acceptable Use Policy when using School Technology.

4.2 Pupils and staff require individual user names and passwords to access the School's internet, intranet and email system which must not be disclosed to any other person. Any pupil or member of staff who has a problem with their user names or passwords must report it immediately to a member of staff in the case of a pupil, or the school's IT provider support desk in the case of an adult.

4.3 No laptop or other mobile electronic device may be connected to the School network without the consent of the Bursar (who will generally consult the School's IT Provider to maintain the integrity of the network). The use of any device connected to the School's network will be logged and monitored by the School's IT provider on behalf of the Bursar and DSL and is subject to the school's Code of Conduct for Staff.

4.4 The School has a separate Wi-Fi connection available for use by visitors to the School. A password, which is changed on a regular basis, must be obtained from a member of staff in order to use the Wi-Fi.

4.5 Use of mobile electronic devices

- 4.5.1 The School has appropriate filtering and monitoring systems in place to protect pupils using the Internet when connected to the School's network. Mobile phones and/or any personal device that can access the internet are banned for pupils at Horris Hill unless specifically allowed for specific occasions.
- 4.5.2 The use of mobile electronic devices by staff is covered in the Staff Code of Conduct, IT Acceptable Use Policy, Social Media Policy, Data Protection Policy for Staff. Unless otherwise agreed in writing, personal mobile devices including laptop and notebook devices should not be used for School purposes except in an emergency.
- 4.5.3 The School's policies apply to the use of Technology by staff and pupils whether on or off School premises and appropriate action will be taken where such use affects the welfare of other pupils or any member of the School community or where the culture or reputation of the School is put at risk.

5 Procedures for dealing with incidents of misuse

5.1 Staff, pupils and parents are required to report incidents of misuse or suspected misuse to the School in accordance with this policy and the School's safeguarding and disciplinary policies and procedures.

5.2 Misuse by pupils

- 5.2.1 Anyone who has any concern about the misuse of Technology by pupils should report it so that it can be dealt with in accordance with the School's Good Behaviour and Sanctions Policy, including the Bullying Policy: Preventing and Tackling where there is an allegation of cyberbullying or in line with the procedures set out in the Peer on Peer Abuse Policy for incidents of online sexual harassment.
- 5.2.2 Anyone who has any concern about the welfare and safety of a pupil must report it immediately in accordance with the School's child protection procedures (see the School's Safeguarding and Child Protection Policy and Procedures).

5.3 Misuse by staff

- 5.3.1 Anyone who has any concern about the misuse of Technology by staff should report it in accordance with the School's Whistleblowing Policy so that it can be dealt with in accordance with the staff disciplinary procedures.
- 5.3.2 If anyone has a safeguarding-related concern, they should report it immediately so that it can be dealt with in accordance with the procedures for reporting and dealing with allegations of abuse against staff set out in the School's Safeguarding and Child Protection Policy and Procedures.

5.4 Misuse by any user

- 5.4.1 Anyone who has a concern about the misuse of Technology by any other user should report it immediately to the Head of Pastoral, Bursar or the Headmaster.
- 5.4.2 The School reserves the right to withdraw access to the School's network by any user at any time and to report suspected illegal activity to the police.

- 5.4.3 If the School considers that any person is vulnerable to radicalisation the school will refer this to the Channel programme. This focuses on support at an early stage to people who are identified as being vulnerable to being drawn into terrorism. Any person who has a concern relating to extremism may report it directly to the police.

6 Monitoring and review

- 6.1 All serious incidents involving the use of Technology will be logged centrally on the Engage database by the DSL and be brought to the attention of the Bursar and Headmaster.
- 6.2 The Designated Safeguarding Lead has responsibility for the implementation and review of this policy and will consider the record of incidents involving the safe use of Technology and the logs of internet activity (including sites visited) as part of the ongoing monitoring of safeguarding procedures, to consider whether existing security and online safety practices within the School are adequate.
- 6.3 Consideration of the effectiveness of the School's online safety procedures and the education of pupils about keeping safe online will be included in the annual review of safeguarding.

Online Safety and Social Media

The DSL takes the lead responsibility for online safety.

The issues within online safety are categorised into four areas of risk

Content, Contact, Conduct, Commerce (risks such as gambling, inappropriate advertising, phishing and/or financial scams. Considering the four Cs (above) will provide the basis of an effective online policy. The school or college should have a clear policy on the use of mobile and smart technology. Amongst other things this will reflect the fact that many children and young people have unlimited and unrestricted access to the internet.

With the current speed of on-line change, some parents and carers have only a limited understanding of online risks and issues. Parents may underestimate how often their children come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond. Some of the risks could be:

- unwanted contact
- grooming
- radicalisation
- online bullying including sharing of nude and or semi-nude images
- digital footprint

The school will therefore seek to provide information and awareness to both pupils and their parents through:

- Curriculum activities and PSHE, including RSHE, to help children to reduce risks, build resilience and raise awareness around staying safe online
- Information included in letters, newsletters, web site
- Parents evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Building awareness around information that is held on relevant web sites and or publications
- Please refer to the school's Online Safety Policy and Social Media Policy.

Cyberbullying

Central to the School's Bullying: Preventing and Tackling Policy is the principle that bullying is always unacceptable and that all pupils have a right not to be bullied.

The school also recognises that it must take note of bullying perpetrated outside school which spills over into the school and so we will respond to any cyber-bullying we become aware of carried out by pupils when they are away from the site.

Cyber-bullying is defined as "an aggressive, intentional act carried out by a group or individual using electronic forms of contact repeatedly over time against a victim who cannot easily defend himself/herself."

By cyber-bullying, we mean bullying by electronic media:

- Bullying by texts or messages or calls on mobile phones
- The use of mobile phone cameras to cause distress, fear or humiliation
- Posting threatening, abusive, defamatory or humiliating material on websites, to include blogs, personal websites, social networking sites
- Using e-mail to message others
- Hijacking/cloning e-mail accounts
- Making threatening, abusive, defamatory or humiliating remarks in on-line forums

Cyber-bullying may be at a level where it is criminal in character. It is unlawful to disseminate defamatory information in any media including internet sites. 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.

The Protection from Harassment Act 1997 makes it an offence to knowingly pursue any course of conduct amounting to harassment.

If we become aware of any incidents of cyberbullying, we will need to consider each case individually as to any criminal act that may have been committed. The school will pass on information to the police if it feels that it is appropriate or are required to do so.

Sharing of nude or semi-nude pictures or video 'Sexting'

'Sexting' often refers to the sharing of nude or semi-nude pictures or video through mobile phones and the internet. It also includes underwear shots, sexual poses and explicit text messaging.

While sharing of nude or semi-nude images often takes place in a consensual relationship between two young people, the use of these images in revenge following a relationship breakdown is becoming more commonplace. The sharing of such images can also be used as a form of sexual exploitation and take place between strangers.

As children as young as 6 years often have access to their own smartphone or tablet, the sharing of nude or semi-nude images is an issue that requires awareness raising across all ages.

The school will use age appropriate educational material to raise awareness, to promote safety and deal with pressure. Parents should be aware that they can come to the school for advice.

Upskirting

In accordance with KCSIE 2021, upskirting is now treated as a criminal offence. Upskirting typically involves taking a picture under a person's clothing without them knowing to obtain sexual gratification or cause them humiliation, distress or alarm. Hampshire Safeguarding Children Partnership safeguarding policy states :

In 2019 the Voyeurism Offences Act came into force and made the practice of upskirting illegal.

Upskirting is defined as someone taking a picture under another person's clothing without their knowledge, with the intention of viewing their genitals or buttocks, with or without underwear. The intent of upskirting is to gain sexual gratification or to cause the victim humiliation, distress or alarm. If this is between pupils, we will follow the peer on peer abuse procedure.

If staff in the school are made aware that upskirting has occurred, then this will be treated as a sexual offence and reported accordingly.

There are behaviours that would be considered as sexual harassment which may be pre-cursors to upskirting. The use of reflective surfaces or mirrors to view underwear or genitals will not be tolerated and the school will respond to these with appropriate disciplinary action and education.

Pupils who place themselves in positions that could allow them to view underwear, genitals or buttocks, will be moved on. Repeat offenders will be disciplined. These locations could include stairwells, under upper floor walkways, outside changing areas and toilets or sitting on the floor or laying down in corridors.

If technology that is designed for covert placement and could be used to take upskirting or indecent images is discovered in the school it will be confiscated. If the technology is in location and potentially may have captured images, this will be reported to the police and left in situ so that appropriate forensic measures can be taken to gather evidence.

Any confiscated technology will be passed to the head teacher to make a decision about what happens to the items and will be carried out under the principles set out in the government guidance on searching, screening and confiscation.

If the image is taken on a mobile phone, the phone will be confiscated under the same principles. This may need to be passed to the police for them to investigate, if there is evidence that a crime has been committed.

Gaming

Online gaming is an activity that the majority of children and many adults get involved in. The school will raise awareness:

- By talking to parents and carers about the games their children play and help them identify whether they are appropriate.
- By supporting parents in identifying the most effective way of safeguarding their children by using parental controls and child safety mode.
- By talking to parents about setting boundaries and time limits when games are played.
- By highlighting relevant resources.

Online reputation

Online reputation is the opinion others get of a person when they encounter them online. It is formed by posts, photos that have been uploaded and comments made by others on people's profiles. It is important that children and staff are aware that anything that is posted could influence

their future professional reputation. The majority of organizations and work establishments now check digital footprint before considering applications for positions or places on courses

Grooming

Online grooming is the process by which one person with an inappropriate sexual interest in children will approach a child online, with the intention of developing a relationship with that child, to be able to meet them in person and intentionally cause harm.

The school will build awareness amongst children and parents about ensuring that the child:

- Only has friends online that they know in real life
- Is aware that if they communicate with somebody that they have met online, that relationship should stay online

That the school will support parents to:

- Recognise the signs of grooming
- Have regular conversations with their children about online activity and how to stay safe online

The school will raise awareness by:

- Running sessions for parents
- Include awareness around grooming as part of their curriculum
- Identifying with parents and children how they can be safeguarded against grooming