Policy Connections

This policy should be read in conjunction with the Supplementary Guidance for policies (covering Philosophy & Ethos; Audience, Monitoring & Evaluation; Assessment, Recording & Reporting; and Supporting Learning Beyond the School) and with the Staff Communication policy, Faculty Guide for Choices, Acceptable User policy, Behaviour Policy, Anti-Bullying policy, Safeguarding and Child Protection policy, the Remote Learning Policy and the Emotional Health and Wellbeing policy.

The aims of the policy are to ensure effective practice in online safety which depends on effective practice in each of the following areas by having

- Effective education for acceptable behaviour by staff and pupils;
- A robust approach to online safety, which empowers, protects and educates the whole school community in its use of technology, including mobile devices, smart technology and artificial intelligence (AI)
- Clear procedures to identify, intervene and escalate an incident, where appropriate
- A comprehensive, agreed and implemented Online Safety Policy;
- A secure, filtered broadband from Lancashire County Council;
- A school network that complies with the National Education Network standards and specifications.

The school recognises that abuse, exploitation, bullying and harmful behaviours can occur online as well as offline. Online concerns will be treated with the same level of seriousness as face-to-face safeguarding concerns and responded to in line with the school's safeguarding and child protection procedures.

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE'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.

The designated safeguarding lead (DSL)

Details of the school's designated safeguarding lead (DSL) and Deputies (DDSLs) are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The DSL 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 and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Ensuring that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged on CPOMS and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- 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
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

Effective Use of Technology

Why the Internet and digital communications are important

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Using technology online will enhance learning

- The school Internet access will be designed expressly for pupil use and will include appropriate filtering.
- 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
- Pupils will be shown how to publish and present information to a wider audience

Pupils will be taught how to evaluate Internet content

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught the importance of cross-checking information before accepting its accuracy.
- Pupils will be taught how to report unpleasant Internet content e.g. by telling an adult.
- The school embeds online safety messages and teaching across the curriculum as a long term whole school approach (EYFS, Primary, Secondary & FE).
- The school recognises that misinformation, disinformation, conspiracy theories and AI-generated or manipulated content present safeguarding risks.
- Pupils will be explicitly taught how to identify unreliable or biased information, recognise AI-generated media such as deepfakes, understand how algorithms and persuasive design can influence beliefs and behaviour, and develop the skills to verify sources and challenge harmful narratives safely. This will be adapted in order to meet the needs and abilties of pupils.

Managing Internet Access for Pupils and Students

Authorising Internet access for pupils and students

- The ICT technician will maintain a current record of all pupils who are granted access to school ICT systems
- For all pupils, access to the Internet will be by adult demonstration with supervised access to specific, approved on-line materials.
- Where appropriate, FE students and parents will be asked to sign the Acceptable Behaviour policy prior to joining the FE Centre.

Enlisting parents' and carers' support

- Parents and carers will be informed of the School's Online Safety Policy via the school Website.
- Parental permission will be sought for the use of pupils' photographs on admission to school. Parents are reminded that they have the right to withdraw consent at any time. Further details can be found in our GDPR policy which is available on the school website.
- The school will maintain a list of online safety resources for parents/carers.
- The school will actively try to engage parents in online safety through targeted events, learner led education and regular communication e.g. facebook and class dojo
- School will inform parents & carers about the school's filtering system Netsweeper

Communications Policy

Introducing the Online Safety Policy to pupils and students

- Guidance about the safe use of technology for pupils will be displayed in classrooms and and on computer devices such as ipads and computers

- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.
- Online Safety training will be embedded across all areas of the school curriculum, including but not limited to, the Computing curriculum, the Personal Social and Health Education (PSHCE) curriculum and the Relationship, Sex and Health Education (RSHE) curriculum (From March 2021), including the Kidsafe programme.

E-mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils will be taught to immediately tell a teacher if they receive an offensive e-mail.
- In e-mail communication, pupils will be taught not to reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school should consider how e-mail from pupils to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.

Managing Social networking and personal publishing for pupils

- The school will control access to social networking sites, and consider how to educate pupils in their safe use. The school's filtering system, **Netsweeper** currently blocks any social network sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be taught to never to give out personal details of any kind that may identify them, their friends or their location.
- Pupils will be taught to use nicknames and avatars when using social networking sites.
- Staff will be vigilant to the potential for pupils to be at risk of being subject to grooming by those with whom they make contact on the internet and will report any concerns to the DSL.
- YouTube is available on SLT, Office Staff, Teaching staff, HLTAs and some TA3's accounts only and access is blocked on all other accounts.
- Pupils' may be asked to use YouTube as part of a structured learning activity, in small groups, where access can be directly monitored. Pupils would not access this in their free time or less structured time.

Managing emerging technologies

- Emerging technologies will be piloted by staff for educational benefit.
- Games machines including the Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering. Care is required in any use in school or other officially sanctioned location.

Artifical Intelligence (AI)

Where Artificial Intelligence (AI) tools are used within school systems or learning activities, the school will ensure that these technologies are risk-assessed prior to use, include appropriate filtering and monitoring, meet data protection and privacy

requirements, and are used under staff supervision. Staff will apply professional judgement when reviewing AI-generated outputs, and pupils will be taught that AI systems may produce inaccurate, biased or manipulated information.

Videoconferencing & webcam use

- Videoconferencing should use the educational broadband network to ensure quality of service and security.
- Videoconferencing would only be part of a planned lesson. Pupils would not access this in their free time or less structured time.
- Pupils must ask permission from the supervising teacher before making or answering a videoconference call.
- Video conferencing and webcam use will be appropriately supervised for the pupils' age and understanding.

Education at Home

- The school recognises that pupils may use ICT more frequently at home. While we cannot apply the same filtering and monitoring systems used in school, we aim to support families by providing guidance and advice to help keep children safe online.
- Staff and parents should be aware that existing policies relating to data protection, safeguarding, image use, and acceptable use of technology remain relevant when pupils access learning at home.
- Home learning is intended to reflect and reinforce activities carried out in school. For example, strategies such as using PECS at lunchtime in school can be supported by parents during mealtimes at home.
- The school can offer information and guidance to support safe ICT use at home; however, responsibility for monitoring and ensuring online safety in the home environment rests with parents and carers.

Use of Mobile Devices by Pupils

All staff should note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.

- Mobile phones, IPods, MP3 players and other devices must be kept in students' lockers during the day and will not be used during lessons or in formal school time. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.
- Only those students who are independent travellers have permission to bring mobile phones in to school and these must be kept in students' lockers during the school day.
- The use of cameras on mobile phones owned by pupils is not permitted in school or any school related activity.

Inappropriate Use of Technology

Our approach to online safety is based on addressing the following categories of risk (also known as the 4 C's).

Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism

Contact – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes

Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and

Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

Content Relating to Suicide and Self-Harm
The school recognises that pupils may encounter online material that references, promotes or encourages suicide and self-harm. This presents a serious safeguarding risk.
In line with Department for Education guidance:

- Exposure to this content will be treated as a **safeguarding concern**
- Staff will avoid sharing or discussing harmful methods or material
- Filtering and monitoring systems help reduce access
- Pupils are taught how to recognise harmful content and seek help
- Concerns are managed in line with the **Safeguarding and Child Protection Policy**, with DSL oversight
- Parents and carers will be informed of concerns, unless staff believe that doing so may place the pupil at further risk, in line with safeguarding procedures.

Online activity of this nature may indicate wider wellbeing needs and will be supported appropriately.

Accidental access
Pupils will be taught that if they access inappropriate materials to:

- Minimise the website / turn the monitor off;
- Tell an adult.

Where a pupil has inappropriately misused technology it is important that this is reported using the school's incident logging procedure, CPOMS*, under the appropriate category. Serious or persistent offences may result in informing parents/carers. Examples of misuse may include:

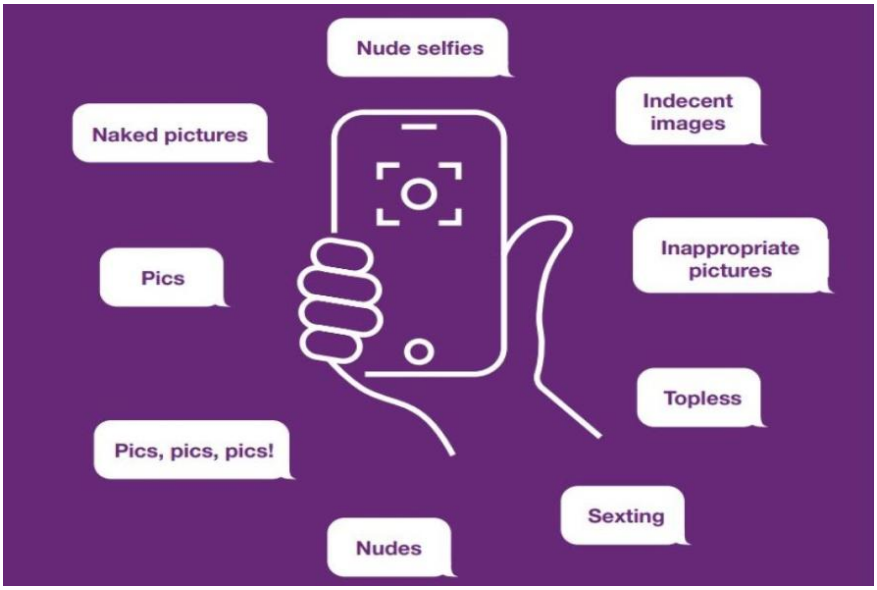
- Accidental access to inappropriate materials;
- Using other people's logins and passwords maliciously;
- Deliberately searching for inappropriate materials;
- Bringing inappropriate electronic files from home;
- Using chats and forums inappropriately.

Technology Assisted Child Sexual Abuse (TA-CSA), Technology Assisted Child Criminal Abuse (TA-CCA and the sending of nude or semi-nude images)
Technology can provide additional routes both to access young people and abuse them. It is essential that pupils and students and parents are taught how to keep

themselves safe when online, at a level that is appropriate to them. Staff have relevant training to deal with incidents of TA-CSA and TA-CCA and any staff made aware of incidents of TA-SCA or TA-CCA should follow the school's safeguarding procedures.

Sharing of nude and semi-nude images
In the latest advice for education settings (UKCIS, 2024), 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. Nudes and semi-nudes can be shared online via social media, gaming platforms, chat apps, forums, or involve sharing between devices using offline services**.**

The term 'nudes' is used as it is most commonly recognised by young people and more appropriately covers all types of image sharing incidents (https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people)



All staff must read the **Responding to the Sharing of Images that are Nude & Semi Nude (Loyne School)** advice and be aware of the 5 points for immediate referral to other agencies (See Appendix 1).

Prevent Duty (Protection of pupils from radicalisation and extremism)
Although serious incidents involving radicalisation have not occurred at the Loyne to date, it is important for us to be constantly vigilant and remain fully informed about the issues which affect the region in which we teach. All staff have relevant training and should ensure that they access refresher training. Staff are reminded to suspend any professional disbelief that instances of radicalisation 'could not happen here' and

refer any concerns through appropriate channels (currently via Designated Senior Leader (DSL)).

Upskirting
Upskirting became a specific criminal offence under the Voyeurism (Offences) Act on 12 April 2019 and is also listed in the 2024 KCSIE document as a form of child on child abuse. It typically involves taking a photograph under a person's clothing without them knowing, with the intention of viewing their genitals or buttocks for sexual gratification or causing humiliation, distress or alarm.
All staff have appropriate training regarding upskirting linked to safeguarding and access regular 'refresher' training. Staff should report any concerns immediatetly to the DSL.

Mental Health
Mental health concerns could signal that a pupil may have suffered, or is at risk of suffering, online abuse, neglect or exploitation. Similarly, online behaviours may indicate that a young person may be experiencing mental health issues. These behaviours coud manifest in overt ways, such as accessing pro-eating disorder websites, or in more subtle ways. All school staff are supported in identifying the signs of mental health issues through relevant training, including annual safeguarding training. When addressing online behaviours or online behavioural changes, staff should take into consideration mental helath concerns as potential underlying factors.

If staff members feel pupils, students or staff are at risk they must follow school reporting procedure and also report online commerce scams to the Anti-Phishing Working Group (https://apwg.org/)

Cybercrime
Cybercrime is criminal activity committed using computers and/or the internet. It is broadly categorised as either 'cyber-enabled' (crimes that can happen off-line but are enabled at scale and at speed on-line) or 'cyber dependent' (crimes that can be committed only by using a computer). Children and young people with particular skill and interest in computing and technology may inadvertently or deliberately stray into cyber-dependent crime. If there are concerns about a child in this area, the designated safeguarding lead (or a deputy), should consider referring into the Cyber Choices programme. Cybercrime should also be addressed or referenced within school and colleges **child protection and safeguarding policies and procedures**.

Examining electronic devices

The headteacher, and any DSL, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from [the headteacher and / or DSL.
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's cooperation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the DSL / headteacher to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Managing Internet Access for Staff

Staff and the Online Safety policy

- All staff will be given the School Online Safety Policy and its importance explained.
- Online Safety training will be included in the mandatory induction programme completed by all new staff.
- Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.

Authorising Internet access for staff

- All staff must read and sign the **Rules for ICT users-staff (LCC)** before using any school ICT resource.
- The ICT technician will maintain a current record of all staff who are granted access to school ICT systems
- Any person not directly employed by the school will be asked to sign an "acceptable behaviour of school ICT" before being allowed to access the internet from the school site.

Managing Social networking and personal publishing for staff

- Staff using Social Networking outside of school must give careful consideration before giving personal contact details to parents/carers who may be 'friends'. Communications with parents, past pupils or siblings of pupils, especially if under the age of 18 should be discouraged.
- Pupils must not be added as 'friends' on any Social Network site. Any comments made by staff on networking sites that bring the school into disrepute may face disciplinary action.

Use of Mobile Devices by Staff

The use of mobile phones is not permitted during the school day other than break times, lunch times or in connection with school business. Mobile phones must not be kept in classrooms or on a person, and instead should be kept in the staffroom or other secure location, e.g. locker.

Staff must use school phone lines or the school mobile to contact parents /carers. Personal mobiles must not be used by staff for this purpose unless there is no alternative, e.g. remote working. In these instances the number must be withheld using 141 and the parent / carer mobile number deleted from the personal handset. There is a designated mobile for the Independent Travel Coordinator to make contact with pupils.

Staff must ensure that they take a mobile phone out with them if they are taking pupils out and about or attending home visits. A school mobile is available from the School Office or, alternatively, personal mobiles can be taken out. However, **UNDER NO CIRCUMSTANCES** must staff access mobile phones when out and about with pupils, whether during the school day or when participating in extended school events, **other than** to make a work related call or in the event of an emergency. The checking of text, email, apps, social media etc is **not permitted.** The safety of our

pupils is paramount and staff must be attentive and vigilant at all times. **Mobile phones must never be used to record or take photos of pupils at any time.**

Security

Information system security

- School ICT systems security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with the Local Authority.

Email

All staff have access to encrypted email. This must be used when sending messages about sensitive issues relating to students or pupils. All staff accounts are secured using two-factor authentication. Refer to the Data Protection Policy for further information.

Assessing risks

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the school nor LCC can accept liability for any material accessed, or any consequences of Internet access.

Managing filtering

- The school will work with the local authority to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils come across unsuitable on-line materials, the site must be reported to the Online Safety Coordinator.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulations 2018.

Published content and the school web site or other on-line space

- Staff or pupil personal contact information will not generally be published. The contact details given online should be kept in the school office.
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupils' images and work

- Photographs / videos of pupils are only taken using school equipment and only for school purposes.
- Pupils full names will not be used anywhere on a school Web site or other on-line space, particularly in association with photographs.
- Written permission from parents or carers will be obtained on admission and at pupils' or students' annual reviews, before photographs of pupils can be published on the school Web site or other on-line space.
- Images of pupils will not refer to the pupil by name.

- Parents should be clearly informed of the school policy on image taking and publishing.

Handling Online Safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure (see schools complaints policy)
- Pupils and parents will be informed of consequences for pupils misusing the Internet.

*Child Protection Online Maintenance System – any incident that concerns a child's wellbeing and/or welfare (including behaviour) is recorded by staff

Reviewed by: Kathryn Veevers & Carla Huddleston
Date: February 2025
Review Date: February 2026

Reviewed by: Kathryn Arts & Carla Huddleston
Date: February 2026
Review Date: February 2027

References and Supporting Documents

Online Safety LCC
https://www.lancashire.gov.uk/youthzone/need-to-know/online-safety/

Prevent Duty
https://www.gov.uk/government/publications/prevent-duty-guidance/revised-prevent-duty-guidance-for-england-and-wales (Updated April 2021)

DfE 'Sexual Violence And Sexual Harassement Between Children In Schools And Colleges' guidance updated 2021
https://www.gov.uk/government/publications/sexual-violence-and-sexual-harassment-between-children-in-schools-and-colleges

DfE 'Sharing Nudes and Semi Nudes-How to Respond to an incident' guidance (December 2020)
https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people/sharing-nudes-and-semi-nudes-how-to-respond-to-an-incident-overview

https://www.gov.uk/government/organisations/uk-council-for-internet-safety

https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer

Appendix 1 – School compliance

Has the school an Online Policy that complies with local authority guidance?	**Y**
Date of latest update (at least annual): **February 2026**	
The school online safety policy was agreed by governors on: **February 2026**	
The policy is available for staff: **staff room, policies folder on shared server, staff portal**	
The policy is available for parents/carers: **on the school website**	
The responsible member of the Senior Leadership Team is: **Kathryn Arts**	
The responsible member of the Governing Body is: **Ann-Marie Houghton**	
The Lead Designated Senior Leader is: **Kathryn Arts**	
Additional DSL's are **Susan Campbell, Emma Flynn & Fiona Gemson**	
The online Coordinator is: **Kathryn Arts / Stewart Atkin**	
Has online training been provided for both pupils and staff?	**Y**
Is there a clear procedure for a response to an incident of concern?	**Y**
Have online materials from the local authority been obtained?	**Y**
Do all staff sign a Code of Conduct for ICT on appointment?	**Y**
Are all pupils aware of the Schools Online Safety Rules?	**Y**
Are online rules displayed in all rooms where computers are used and expressed in a form that is accessible to all pupils?	**Y**
Do parents/carers sign and return an agreement that their child will comply with the School Online Rules?	**Yes for appropriate pupils**
Are staff, pupils, parents/carers and visitors aware that network and Internet use is closely monitored and individual usage can be traced?	**Y**
Has an ICT security audit been initiated by SLT, possibly using external expertise?	**Y**
Is personal data collected, stored and used according to the principles of the Data Protection Act?	**Y**
Is Internet access provided by an approved educational Internet service provider which complies with DCSF requirements (e.g. KCN, Regional Broadband Consortium, NEN Network)?	**Y**
Has the school-level filtering been designed to reflect educational objectives and approved by SLT?	**Y**

Appendix 2 – Responding to the sharing of images: Advice for all school staff

Responding to the Sharing of Images (Nude & Semi Nude)

The following guidance is taken from
https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people
Department for Education (2024)

Initial disclosure:
This could come from a pupil directly, a parent, a pupil's friend.

Initial review with safeguarding team:

At this initial stage the safeguarding team review the information and consider the 5 points for immediate referral. They make an initial decision about **whether the incident can be dealt with in house**.

5 points for referral:
1. **Adult involvement**
2. **Coercion or blackmail**
3. **Extreme or violent**
4. **Under 13**
5. **Immediate risk of harm**

Risk assessment/Dealing with the incident:

Consider the risk of harm and at any point if there are 'causes for concern' you can refer out to police/social care.

Social Care/MASH referral
Refer to local arrangements for dealing with incidents and contact local services.

If a referral to the Police is required this should be done via Social Care/ MASH

Management in school:

Ensure parents are informed and the incident recorded **following all child protection and safeguarding procedures**.

Frequently Asked Questions

Q: Do I need to report all instances of sharing nude or semi nude images to the Police and/or Children's Social Care?
No, the Initial Review Meeting should consider whether immediate referral is required according to the 5 criteria above. If none of these criteria apply, schools may therefore decide it is appropriate to manage the incident locally.

Q: As the DSL, am I allowed to view the image in order to make a decision?
https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-peopleclear examples of circumstances when it may be necessary to view imagery and what actions the DSL should/should not take.

Q: Should I involve parents/carers?
The guidance highlights that "Parents should be informed at an early stage and involved in the process unless there is good reason to believe that involving parents would put the young person at risk of harm". Government advice includes guidance around supporting victims and steps that can be taken to get images removed

Q: Will the young person get a criminal record if the incident is reported to the police?
This will depend upon the circumstances and any incidents reported to the Police will require recording and an investigation (although this is not the same as having a criminal record). Where appropriate, the Police may decide it is not in the public interest to pursue an investigation.

Appendix 3 – Permissable use of technology in school

Communication Technologies	Staff & other adults				Pupils & Students			
	Allowed	Allowed in the staffroom & staff office	Allowed for selected staff	Not Allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	✓						✓	
Use of mobile phones in lessons				✓				✓
Use of mobile phones in break time		✓						✓
Taking photos on mobile phones or personal camera devices				✓				✓
Use of personal hand held devices		✓						✓
Use of personal email account in school, or on school network				✓				✓
Use of school email for personal emails				✓				✓
Use of chat rooms / facilities				✓				✓
Use of instant messaging		✓						✓
Use of social networking sites		✓						✓
Use of personal blogs				✓				✓
Use of educational blogs	✓						✓	