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, Computing Policy, Acceptable Behaviour policy and Anti-Bullying policy, Safeguarding and Child Protection policy. Remote Learning Policy (pending governors approval)

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

- Education for acceptable behaviour by staff and pupils;
- A comprehensive, agreed and implemented Online Safety Policy;
- Secure, filtered broadband from Lancashire County Council;
- A school network that complies with the National Education Network standards and specifications.

Teaching and learning

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.

Internet use 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. For online teaching activities on Online Safety visit http://www.lancsngfl.ac.uk/onlinesafety/index.php?category_id=3
- 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.

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 in newsletters, the school brochure and 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

Communications Policy

Introducing the Online Safety Policy to pupils and students

- Online Safety rules, in an appropriate format using Communicate In Print, will be posted in all rooms where computers are used and discussed with pupils regularly.
- 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.

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

- Following the increased use of blended learning, as a result of the Covid-19 pandemic, guidance and training is available to staff and parents, which supports them in keeping pupils safe online, in the event of periods of blended learning.
- Staff and parents are advised that existing policies in relation to data protection, child protection, image use and acceptable use of technology still apply in blended learning situations.

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

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 Sexting

Technology can provide additional routes both to access young people and abuse them. It is essential that pupils and students 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.

Sexting

Sexting is the sharing of sexually suggestive photos or videos via mobile or internet. It is important to note that sexting is often the result of young people's natural curiosity about sex and relationships and that pupils and students need education, support and safeguarding, not criminalisation.

All staff must read the **Responding to Sexting (Loyne School)** advice and be aware of the 5 points for immediate referral to other agencies (See Appendix 1).

Guidance on how to deal with sexting can be found at:
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/551575/6.2439_KG_NCA_Sexting_in_Schools_WEB__1_.PDF

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 2019 KSCIE document as a form of peer on peer 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.

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.
- 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

Staff must use school phone lines or the school mobile to contact pupils. Personal mobiles must not be used by staff for this purpose. 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
SLT, Office staff and Teaching staff have access to encrypted mail. This should be used when sending mail regarding sensitive issues related to students and pupils at school.

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 and NAACE 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: Ciara Davies
Date: January 2021
Review Date: February 2022

References
Lancashire e safety Guidance Document
http://www.lancsngfl.ac.uk/esafety/download/file/Primary%20eSafety%20Guidance%20Document%20November%202010.pdf

Lancashire Primary eSafety Framework Document
http://www.lancsngfl.ac.uk/esafety/index.php?category_id=13
DfE Keeping children safe in education Statutory guidance for schools and colleges (September 2020) Annex C Online Safety
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/912592/Keeping_children_safe_in_education_Sep_2020.pdf
Prevent Duty
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/439598/prevent-duty-departmental-advice-v6.pdf
DfE 'Safeguarding and Remote Education during Covid-19' guidance for schools and colleges
https://www.gov.uk/guidance/safeguarding-and-remote-education-during-coronavirus-covid-19

Has the school an Online Policy that complies with local authority guidance?	**Y**
Date of latest update (at least annual):-**January 2021**	
The school online safety policy was agreed by governors on: **October 2018**	
The policy is available for staff: **staff room, policies folder on shared server**	
The policy is available for parents/carers: **on the school website**	
The responsible member of the Senior Leadership Team is: **Julie McGrath/Susan Campbell**	
The responsible member of the Governing Body is: **Amanda Gardner**	
The Lead Designated Senior Leader is: **Kathryn Veevers**	
Additional DSL's are **Julie McGrath, Susan Campbell & Fiona Gemson**	
The online Coordinator is: **Stewart Atkin / Ciara Davies**	
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 / NAACE been obtained?	**Y**
Do all staff sign a Code of Conduct for ICT on appointment?	**Y**
Are all pupils aware of the Schools e-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 1

Responding to Sexting

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**.

(For more information see page 13 of UKCCIS Sexting in schools and colleges)

5 points for referral:

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

(For more information refer to section 2 of UKCCIS Sexting in schools and colleges)

Risk assessment/Dealing with the incident:

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

(For more information refer to page 14 and Annex A of UKCCIS Sexting in schools and colleges)

Police/Social Care/MASH referral

Refer to your local arrangements for dealing with incidents and contact local services.

(For more information refer to page 17of UKCCIS Sexting in schools and colleges)

Management in school:

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

(For more information see page 14 of UKCCIS Sexting in schools and colleges)

Frequently Asked Questions

Q: Do I need to report all Sexting instances 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?
The section 'Searching devices, viewing and deleting imagery' on Pages 15 & 16 of the UKCCIS guidance provides clear 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 when dealing with Sexting instances?
Page 10 of the UKCCIS 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". Guidance on Pages 31-34 and 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 I refer the incident to the Police?

This will depend upon the circumstances and all Sexting 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 and further detailed information about this aspect and the Police response can be found on Pages 8 & 9 of the UKCCIS guidance.