E-Safety Policy

Reviewed:

January 2023

The E-Safeguarding policy is part of the computing policy and School Development plan with a relation to other policies that include those for behaviour, personal, social and health education and citizenship. The e-Safeguarding Policy and its implementations will be reviewed annually.

The appointed eSafeguarding Coordinator is Laura Duffy in conjunction with the school DSL Emma Jones. Our eSafeguarding Policy has been written by the school, building on the Wakefield eSafeguarding Policy and in line with the 'Keeping Children Safe in Education' 2019 (KCSIE) now updated with KCSIE 2022. It has been agreed by senior management and approved by governors.

Aims

This policy aims to:

- Set out expectations for all Ryhill Junior, Infant and Nursery School community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)
- Help all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, and regardless of device or platform
- Facilitate the safe, responsible and respectful use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online
- Help school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
- for the protection and benefit of the children and young people in their care, and
- for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice
- for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession
- Establish clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as Behaviour Policy or Anti-Bullying Policy)

How will this policy be communicated?

This policy can only impact upon practice if it is a (regularly updated) living document. It must be accessible to and understood by all stakeholders. It will be communicated in the following ways:

- Posted on the school website.
- Available on the staff network/drive.
- Part of school induction pack for all new staff (including temporary, supply and non-classroom based staff)
- Integral to safeguarding updates and training for all staff.

- Clearly reflected in the Acceptable Use Policies (AUPs) for all staff, volunteers, contractors, governors, pupils, parents/carers.
- AUPs issued to whole school community, on entry to the school, with annual reminders of where to find them if unchanged, and reissued if updated after annual review.
- Reviews of this online-safety policy will include input from staff, pupils and other stakeholders, helping to ensure further engagement.

Roll of the designated Online Safety Lead

Key responsibilities

- Where the online-safety coordinator is not the named DSL or deputy DSL, ensure there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised
- Ensure an effective approach to online safety that empowers the school to protect and educate the whole school community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate.
- Liaise with the local authority and work with other agencies in line with Working together to safeguard children.
- Take day to day responsibility for online safety issues and be aware of the potential for serious child protection concerns
- Work with the headteacher, DPO and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Stay up to date with the latest trends in online safety.
- Review and update this policy, other online safety documents and the strategy on which they are based and submit for review to the governors/trustees.
- Receive regular updates in online safety issues and legislation, be aware of local and school trends.
- Ensure that online safety education is embedded across the curriculum (e.g. by use of the UKCIS framework 'Education for a Connected World') and beyond, in wider school life
- Promote an awareness and commitment to online safety throughout the school community, with a strong focus on parents, who are often appreciative of school support in this area, but also including hard-to-reach parents
- Liaise with school technical, pastoral, and support staff as appropriate.
- Communicate regularly with SLT and the designated safeguarding and online safety governor/committee to discuss current issues, review incident logs and filtering/change control logs.
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident.
- Oversee and discuss 'appropriate filtering and monitoring' and ensure staff are aware.

- Ensure the 2021 DfE guidance on sexual violence and harassment is followed throughout the school and that staff adopt a zero-tolerance approach to this, as well as to bullying.
- Facilitate training and advice for all staff:
- All staff must read KCSIE Part 1 and all those working with children Annex A.
- All staff to be aware of Annex C (online safety).
- Cascade knowledge of risks and opportunities throughout the organisation.

Roll of the Computing Lead: Mrs L Duffy

- As listed in 'all staff' section.
- Oversee the delivery of the online safety element of the computing curriculum in accordance with the national curriculum.
- Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements

An overview of the roles and responsibilities of the students, staff Governors and Parent volunteers.

Key Responsibilities:

- A planned eSafeguarding programme will be provided as part of our cyber – bullying information, through E-Safety lessons, this will cover both the use of computers and new technologies in school and outside school.
- Key eSafeguarding messages will be addressed through a planned programme of computing lessons, PSHE lessons and Picture News assemblies.
- Pupils will be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils will be helped to understand the pupil AUP.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.
- Understand that online safety is a core part of safeguarding; as such it is part of everyone's job – never think that someone else will pick it up
- Know who the Designated Safeguarding Lead (DSL) and Online Safety Lead (OSL) are. (DSL: E Jones OSL: L Duffy)
- Read Part 1, Annex A and Annex C of Keeping Children Safe in Education
- Read and follow this policy in conjunction with the school's main safeguarding policy.
- Record online-safety incidents in the same way as any safeguarding incident and report in accordance with school procedures.
- Understand that safeguarding is often referred to as a jigsaw puzzle – you may have discovered the missing piece so do not keep anything to yourself
- Sign and follow the staff acceptable use policy.
- Notify the DSL/OSL if policy does not reflect practice in your school and follow escalation procedures if concerns are not promptly acted upon.

- Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in school or setting as homework tasks, encourage sensible use, monitor what pupils/students are doing and consider potential dangers and the age appropriateness of websites (ask your DSL what appropriate filtering and monitoring policies are in place)
- To carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law.
- Prepare and check all online source and resources before using within the classroom.
- Encourage pupils to follow their acceptable use policy, remind them about it and enforce school sanctions.
- Notify the DSL/OSL of new trends and issues before they become a problem.
- Receive regular updates from the DSL/OSL and have a healthy curiosity for online safety issues.
- Model safe, responsible and professional behaviours in your own use of technology. This includes outside the school hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff.

Roll of the Network Technician: Mint Support Ltd

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- Work closely with the designated safeguarding lead / online safety lead / data protection officer to ensure that school systems and networks reflect school policy
- Ensure the above stakeholders understand the consequences of existing services and of any changes to these systems (especially in terms of access to personal and sensitive records / data and to systems such as YouTube mode, web filtering settings, sharing permissions for files on cloud platforms etc)
- Support and advice on the implementation of 'appropriate filtering and monitoring' as decided by the DSL and senior leadership team.
- Maintain up-to-date documentation of the school's online security and technical procedures.
- To report online-safety related issues that come to their attention in line with school policy.
- Manage the school's systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls.

- Monitor the use of school technology, online platforms and social media presence and that any misuse/attempted misuse is identified and reported in line with school policy.

How will the policy be introduced to pupils?

As pupils' perceptions of the risks will vary; the eSafeguarding rules will need to be explained or discussed at the start of each school year. There are safety posters with the eSafeguarding rules on which are located around school and in classrooms. This will be discussed with the children, on a regular basis before a computing lesson begins.

Useful eSafeguarding programmes include:

Think U Know www.thinkuknow.co.uk/

Grid Club www.gridclub.com

The BBC Chat Guide www.bbc.co.uk/chatguide/

How will parents' support be enlisted?

Many parents and carers have only a limited understanding of eSafeguarding risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it.

Internet use in pupils' homes is increasing rapid, encouraged by offers of free access and continual media coverage. Unless parents are aware of the dangers, pupils may have unrestricted access to the Internet. Leaflets are given out to the children with eSafeguarding guidance on and what to look out for when their child has access to the Internet. Parents are advised to check if their child's use elsewhere is covered by an appropriate use policy. Parents' attention will be drawn to the school's eSafeguarding Policy in newsletters, the school brochure and on the school website. Internet issues will be handled sensitively, and parents will be advised accordingly. Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents. Parents will be made aware that videos and still photographs taken by themselves are to be used for personal use only.

Staff training with the E-Safeguarding Policy

A planned programme of formal eSafeguarding training will be made available to staff, as part of the safeguarding programme, included extended schools staff. All new staff should receive eSafeguarding training as part of their induction programme, ensuring that they fully understand the school eSafeguarding policy and Acceptable Use Policies. The eSafeguarding policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days/Governors meetings. The eSafeguarding Coordinator will provide advice / guidance / training as required to individuals as required

Governor training and the E-Safeguarding policy

Governor training will be offered through the attendance at staff INSET days, Governor Services and Bespoke training when available.

Education and the curriculum.

Why is Internet use so important?

The rapid developments in electronic communications are having many effects, some profound, on society. Now every pupil is younger than the World Wide Web and many use it more than teachers. Nevertheless it is important to state what we are trying to achieve in education through computing and Internet use.

- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the schools management functions.
- Internet use is part of the statutory curriculum and a necessary tool for learning.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.
- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and the various types of content and to take care of their own safety and security.

How does Internet use benefit education?

- Children will have access to worldwide educational resources including museums and art galleries.
- Inclusion in the National Education Network, which connects all UK schools.
- Educational and cultural exchanges between pupils worldwide.
- Vocational, social and leisure use in libraries, clubs and at home.
- Access to experts in many fields for pupils and staff.
- Professional development for staff through access to national developments, educational materials and effective curriculum practice.
- Collaboration across support services and professional associations.
- Improved access to technical support including remote management of networks and automatic system updates.
- Access to learning wherever and whenever convenient.

How can Internet use enhance learning?

The school Internet access has been designed expressly for pupils use and includes the filtering systems of; **Sophos**, **Windows defender** and a **firewall**. Pupils are taught what Internet use is acceptable and what is not and given clear objectives for Internet use. It is planned to enrich and extend learning activities and access levels which are reviewed to reflect the curriculum requirements and age of the pupils. Staff give pupils on-line activities that support the learning outcomes planned for the pupil's age and maturity. Throughout school pupils will be educated in the effective use of the Internet and Internet research.

The following subjects have the clearest online safety links:

- PSHE
- Relationships education, relationships and sex education (RSE) and health
- Computing
- Citizenship

However, as stated in the role descriptors above, it is the role of all staff to identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils)

Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in school or setting as homework tasks, all staff should encourage sensible use, monitor what pupils/students are doing and consider potential dangers and the age appropriateness of websites.

Equally, all staff should carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law. saferesources.lgfl.net has regularly updated theme-based resources, materials and signposting for teachers and parents.

At Ryhill Junior, Infant and Nursery School we recognise that online safety and broader digital resilience must be thread throughout the curriculum and that is why we are working to adopt the cross-curricular framework 'Education for a Connected World' from UKCIS (the UK Council for Internet Safety).

How should personal data be protected?

The quantity and variety of data held on pupils, families and on staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused. The Data Protection Act 2018 controls how your personal information is used by organisations, businesses or the government. The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR). Everyone responsible for using personal data has to follow strict rules called 'data protection principles'. They must make sure the information is:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary

- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

How will Internet access be authorised?

The school has allocated Internet access for staff and pupils on the basis of educational need. It is clear who has Internet access and who has not. The school will maintain a current record of all staff and pupils who are granted access to the schools electronic communications. At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.

What are the risks of Internet use?

- Receiving inappropriate content
- Grooming
- Requests for personal information
- Viewing "incitement" sites
- Bullying and threats
- Identity theft
- Publishing inappropriate content
- Online gambling
- Misuse of computer systems
- Publishing personal information
- Hacking and security breaches
- Corruption or misuse of data

How will risks be assessed?

As the quantity and breadth of information available through the Internet continues to grow it is not possible to guard against every undesirable situation. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor WDC can accept liability for the material accessed, or any consequences resulting from Internet use. The school audits the technologies used to establish if the eSafeguarding policy is adequate and that the implementation of the eSafeguarding policy is appropriate. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

How will eSafeguarding complaints be handled?

It is vital that all staff recognise that online-safety is a part of safeguarding (as well as being a curriculum strand of Computing, PSHE/RSE and Citizenship). General concerns must be handled in the same way as any other safeguarding concern; safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should talk to the online-safety lead / designated safeguarding lead to contribute to the overall picture or highlight what might not yet be a problem. Support staff will often have a unique insight and opportunity to find out about issues first in the playground, corridors, toilets and other communal areas outside the classroom (particularly relating to bullying and sexual harassment and violence).

School procedures for dealing with online-safety will be mostly detailed in the following policies (primarily in the first key document):

- Safeguarding and Child Protection Policy
- Sexual Harassment / Peer on Peer Abuse Policy
- Anti-Bullying Policy
- Behaviour Policy (including school sanctions)
- Acceptable Use Policies
- Prevent Risk Assessment / Policy
- Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc)

This school commits to take all reasonable precautions to ensure online safety, but recognises that incidents will occur both inside school and outside school (and that those from outside school will continue to impact on pupils when they come into school.) All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes.

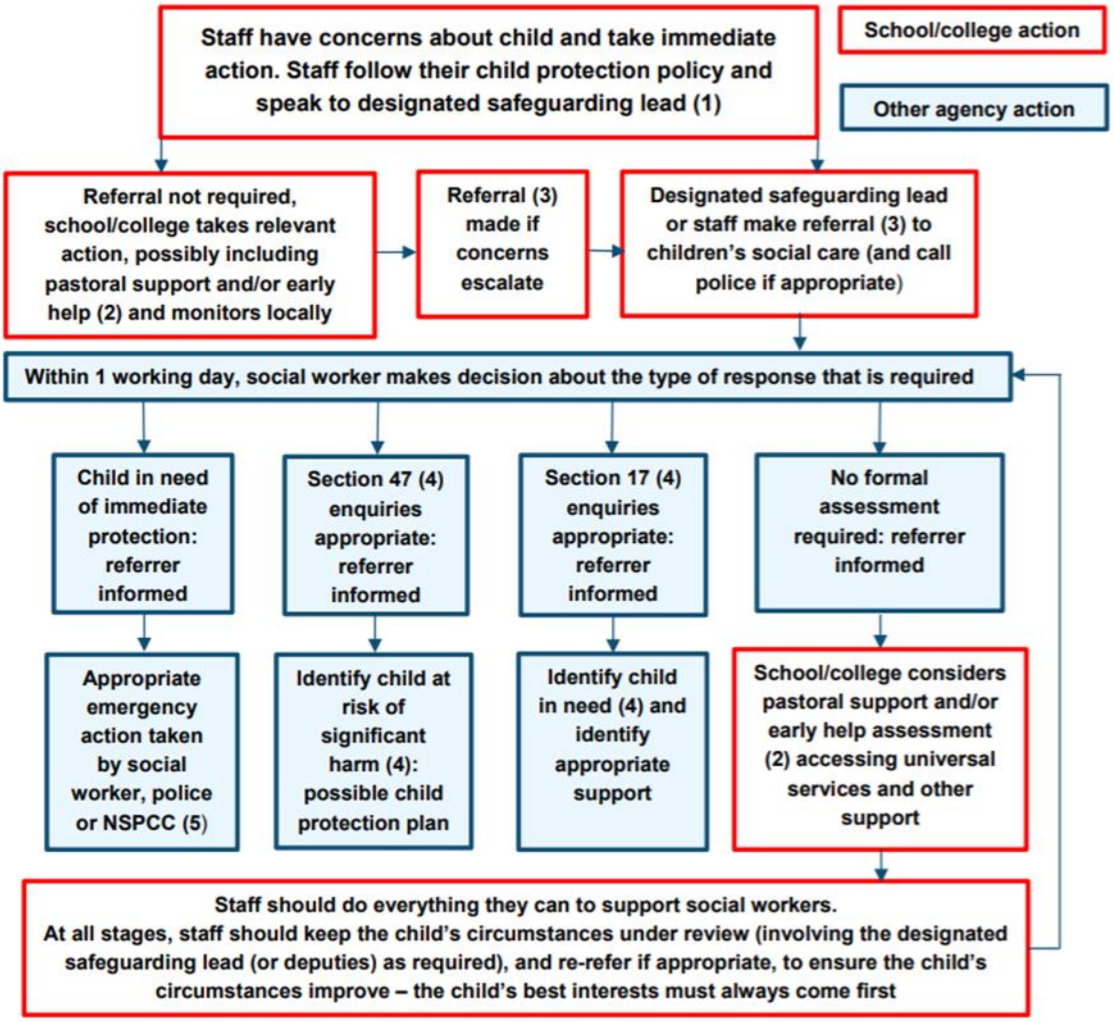
Any suspected online risk or infringement should be reported to the online safety lead / designated safeguarding lead on the same day – where clearly urgent, it will be made by the end of the lesson.

Any concern/allegation about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the compliant is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer). Staff may also use the NSPCC Whistleblowing Helpline.

The school will actively seek support from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline, NCA CEOP, Prevent Officer, Police, IWF). We will inform parents/carers of online-safety incidents involving their children, and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly disturbing or breaks the law (particular procedures are in place for sexting and upskirting; see section below).

Actions where there are concerns about a child.

The following flow chart is taken from Keeping Children Safe in Education 2022 as the key education safeguarding document. As outlined previously, online safety concerns are no different to any other safeguarding concern.



Staff have concerns about child and take immediate action. Staff follow their child protection policy and speak to designated safeguarding lead (1)

School/college action

Other agency action

Referral not required, school/college takes relevant action, possibly including pastoral support and/or early help (2) and monitors locally

Referral (3) made if concerns escalate

Designated safeguarding lead or staff make referral (3) to children's social care (and call police if appropriate)

Within 1 working day, social worker makes decision about the type of response that is required

Child in need of immediate protection: referrer informed

Section 47 (4) enquiries appropriate: referrer informed

Section 17 (4) enquiries appropriate: referrer informed

No formal assessment required: referrer informed

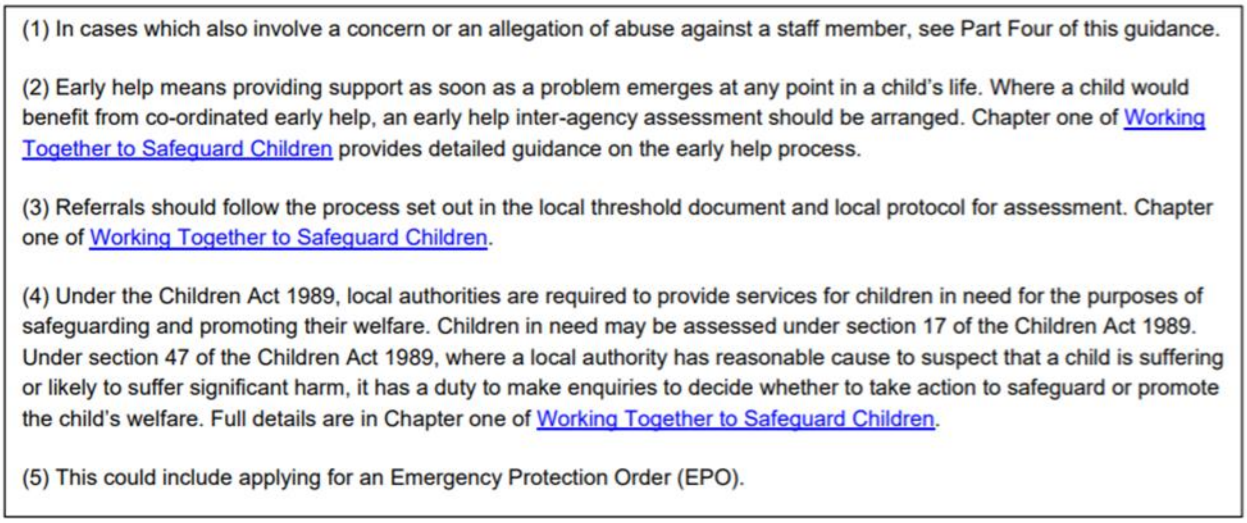
Appropriate emergency action taken by social worker, police or NSPCC (5)

Identify child at risk of significant harm (4): possible child protection plan

Identify child in need (4) and identify appropriate support

School/college considers pastoral support and/or early help assessment (2) accessing universal services and other support

Staff should do everything they can to support social workers.
At all stages, staff should keep the child's circumstances under review (involving the designated safeguarding lead (or deputies) as required), and re-refer if appropriate, to ensure the child's circumstances improve – the child's best interests must always come first



(1) In cases which also involve a concern or an allegation of abuse against a staff member, see Part Four of this guidance.

(2) Early help means providing support as soon as a problem emerges at any point in a child's life. Where a child would benefit from co-ordinated early help, an early help inter-agency assessment should be arranged. Chapter one of Working Together to Safeguard Children provides detailed guidance on the early help process.

(3) Referrals should follow the process set out in the local threshold document and local protocol for assessment. Chapter one of Working Together to Safeguard Children.

(4) Under the Children Act 1989, local authorities are required to provide services for children in need for the purposes of safeguarding and promoting their welfare. Children in need may be assessed under section 17 of the Children Act 1989. Under section 47 of the Children Act 1989, where a local authority has reasonable cause to suspect that a child is suffering or likely to suffer significant harm, it has a duty to make enquiries to decide whether to take action to safeguard or promote the child's welfare. Full details are in Chapter one of Working Together to Safeguard Children.

(5) This could include applying for an Emergency Protection Order (EPO).

Sexting

All schools should refer to the UK Council for Internet Safety (UKCIS) guidance on sexting (also referred to as 'youth produced sexual imagery') in schools. NB - where one of the parties is over 18, this is no longer sexting but child sexual abuse.

There is a one-page overview called Sexting; how to respond to an incident for all staff (not just classroom-based staff) to read, in recognition of the fact that it is mostly someone other than the designated safeguarding lead (DSL) or online safety lead to first become aware of an incident, and it is vital that the correct steps are taken. Staff other than the DSL must not attempt to view, share or delete the image or ask anyone else to do so, but to go straight to the DSL. The school DSL will in turn use the full guidance document, Sexting in Schools and Colleges to decide next steps and whether other agencies need to be involved. It is important that everyone understands that whilst sexting is illegal, pupils/students can come and talk.

Upskirting

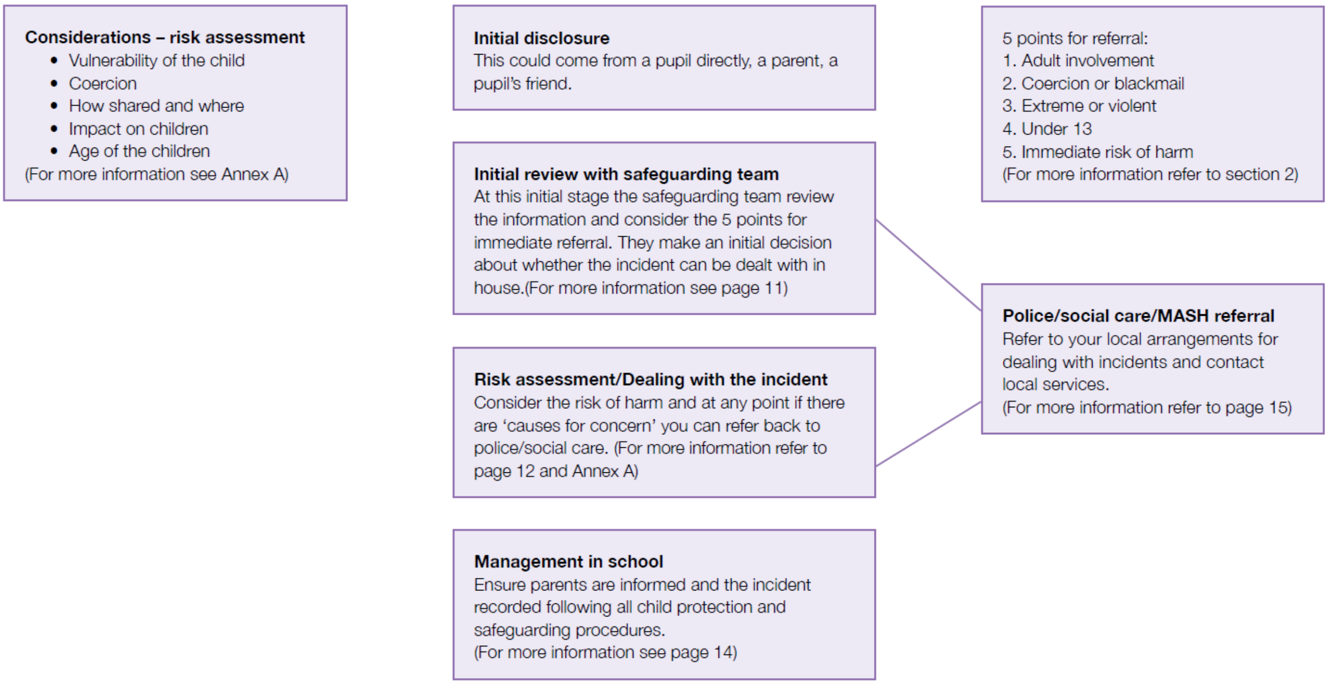
It is important that everyone understands that upskirting (taking a photo of someone under their clothing) is now a criminal offence, as highlighted in Keeping Children Safe in Education and that pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area.

Bullying

Online bullying should be treated like any other form of bullying and the school bullying policy should be followed for online bullying, which may also be referred to as cyber bullying.

Annex G

Flowchart for responding to incidents



Considerations – risk assessment
- Vulnerability of the child
- Coercion
- How shared and where
- Impact on children
- Age of the children

(For more information see Annex A)

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 11)

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 12 and Annex A)

Management in school
Ensure parents are informed and the incident recorded following all child protection and safeguarding procedures.
(For more information see page 14)

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)

Police/social care/MASH referral
Refer to your local arrangements for dealing with incidents and contact local services.
(For more information refer to page 15)

Sexual Violence and Harassment

DfE guidance on sexual violence and harassment is referenced in Keeping Children Safe in Education and also a document in its own right. Paragraphs 45-49 cover the immediate response to a report and confidentiality which is highly relevant for all staff; the case studies section provides a helpful overview of some of the issues which may arise.

Any incident of sexual harassment or violence (online or offline) should be reported to the DSL who will follow the full guidance. Staff should work to foster a zero-tolerance culture. The guidance stresses that schools must take all forms of sexual violence and harassment seriously, explaining how it exists on a continuum and that behaviours incorrectly viewed as 'low level' are treated seriously and not allowed to perpetuate. The document makes specific reference to behaviours such as bra-strap flicking and the careless use of language.

Misuse of school technology (devices, systems, networks or platforms)

Clear and well communicated rules and procedures are essential to govern pupil and adult use of school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

These are defined in the Acceptable Use Policy as well as in this document, for example in the sections relating to the professional and personal use of school platforms / networks / clouds, devices and other technology, as well as to BYOD (bring your own device) policy.

Where pupils contravene these rules, the school behaviour policy will be applied; where staff contravene these rules, action will be taken as outlined in the staff code of conduct/handbook.

Further to these steps, the school reserves the right to withdraw – temporarily or permanently – any or all access to such technology, or the right to bring devices onto school property.

Social Media Incidents

See the social media section later in this document for rules and expectations of behaviour for children and adults in the Ryhill Junior, Infant and Nursery School community. These are also governed by school Acceptable Use Policies.

Breaches will be dealt with in line with the school behaviour policy (for pupils) or code of conduct / handbook (for staff).

Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community, Ryhill Junior, Infant and Nursery School will request that the post be deleted and will expect this to be actioned promptly.

Where an offending post has been made by a third party, the school may report it to the platform it is hosted on, and may contact the Professionals' Online Safety Helpline (run by the UK Safer Internet Centre) for support or help to accelerate this process.

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also ensure that the relevant people named in the above sections will be effective in carrying out their eSafeguarding responsibilities:

- The schools IT systems will be managed in ways that ensure the school meets any eSafeguarding technical requirements and any relevant Local Authority eSafeguarding Policy and guidance.
- There will be regular reviews and audits of the safety and security of school IT systems. Servers, wireless systems and cabling will be securely located and physical access restricted.
- All users will have clearly defined access rights to school IT systems. The Network will record details of the access rights available to groups of users.
- The "master/administrator" passwords for the school IT system, used by the Network Manager will also be available for the Head and kept in a secure place
- Users will be made responsible for the security of their username and password and must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that this is known to others.
- Any filtering issues should be reported immediately to the LA, who can then subsequently escalate these to the YHGfL support centre.
- Requests from staff for sites to be removed or added from the filtered feed will be considered by the Head teacher and if the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the headteacher.
- Appropriate and relevant security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- Guest and Student accounts are in place with usernames and passwords. These accounts are regularly checked and saved work deleted when no longer in use.
- An acceptable use agreement is in place regarding the extent of personal use that users (staff / students / pupils / community users) are allowed on laptops and other portable devices that may be used out of school. These must not be connected to the Internet outside school and only the named user of that laptop is allowed access.
- The acceptable use agreement is in place that forbids staff from installing personal programmes on school workstations/portable devices without the consent from either the Server Manager, Computing Co-ordinator or Head teacher.
- The acceptable use agreement is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school workstations / portable devices. Personal equipment within school is in addition forbidden.
- The school infrastructure and individual workstations are protected by up to date virus software.

- Personal data cannot be sent over the Internet or taken off the school site unless safely encrypted or otherwise secured.

Electronic communications

Email

Staff at this school use Microsoft 365 system for all school emails. This system is fully auditable, trackable and managed by Mint Support Ltd on behalf of the school. This is for the mutual protection and privacy of all staff, pupils and parents, as well as to support data protection.

General principles for email use are as follows:

- Email is Microsoft 365 the only means of electronic communication to be used between staff. Use of a different platform must be approved in advance by the data-protection officer / headteacher in advance.
- Class Dojo is the only means of electronic communication to be used between staff and parents.
- Any unauthorised attempt to use a different system may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).
- Email may only be sent using the email systems above. There should be no circumstances where a private email is used; if this happens by mistake, the DSL/Headteacher/DPO (the particular circumstances of the incident will determine whose remit this is) should be informed immediately.
- Staff or pupil personal data should never be sent/shared/stored on email.
- If data needs to be shared with external agencies it must be encrypted.
- Appropriate behaviour is expected at all times, and the system should not be used to send inappropriate materials or language which is or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring the school into disrepute or compromise the professionalism of staff
- Staff are NOT allowed to use the email system for personal use and should be aware that all use is monitored, their emails may be read and the same rules of appropriate behaviour apply at all times. Emails using inappropriate language, images, malware or to adult sites may be blocked and not arrive at their intended destination.
- See also the social media section of this policy.

School Website

The school website is a key public-facing information portal for the school community (both existing and prospective stakeholders) with a key reputational value. Where other staff submit information for the website, they are asked to remember:

- School has the same duty as any person or organisation to respect and uphold copyright law – schools have been fined thousands of pounds for copyright breaches. Sources must always be credited and material only used with permission.

- Where pupil work, images or videos are published on the website, their identities are protected and full names are not published (remember also not to save images with a filename that includes a pupil's full name).

Cloud Platforms

Ryhill Junior, Infant and Nursery School adheres to the principles of the DfE document 'Cloud computing services: guidance for school leaders, school staff and governing bodies'. The following principles apply:

- Privacy statements inform parents and children (13+) when and what sort of data is stored in the cloud
- The DPO approves new cloud systems, what may or may not be stored in them and by whom. This is noted in a DPIA (data-protection impact statement) and parental permission is sought.
- Regular training ensures all staff understand sharing functionality and this is audited to ensure that pupil data is not shared by mistake. Open access or widely shared folders are clearly marked as such.
- Staff are only given access and/or sharing rights when they can demonstrate an understanding of what data may be stored and how it can be seen.
- Two-factor authentication is used for access to staff or pupil data
- Pupil images/videos are only made public with parental permission.
- Only school-approved platforms are used by students or staff to store pupil work.
- All stakeholders understand the difference between consumer and education products (e.g. a private Gmail account or Google Drive and those belonging to a managed educational domain)

Digital images and Video

When a pupil joins the school, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos, for what purpose (beyond internal assessment, which does not require express consent) and for how long. Parents answer as follows:

- For displays around the school
- For the newsletter
- For use in paper-based school marketing
- For online prospectus or websites
- For a specific high profile image for display or publication
- For social media

Whenever a photo or video is taken/made, the member of staff taking it will check the latest database before using it for any purpose. Any pupils shown in public facing materials are never identified with more than first name (and photo file names/tags do not include full names to avoid accidentally sharing them). All staff are governed by their contract of employment and the school's Acceptable Use Policy, which covers the use of mobile phones / personal equipment for taking pictures of pupils, and where these are stored. At Ryhill Junior, Infant and Nursery School no member of staff will ever use their personal phone to capture photos or videos of pupils. Photos are stored on the school network in line with the retention schedule of the school Data Protection Policy.

Staff and parents are reminded annually about the importance of not sharing without permission, due to reasons of child protection (e.g. looked-after children often have restrictions for their own protection), data protection, religious or cultural reasons, or simply for reasons of personal privacy.

We encourage young people to think about their online reputation and digital footprint, so we should be good adult role models by not oversharing (or providing embarrassment in later life – and it is not for us to judge what is embarrassing or not).

Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children

Pupils are advised to be very careful about placing any personal photos on social media. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they / or a friend are subject to bullying or abuse.

Social Media

Social media (including all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a school, we accept that many parents, staff and pupils will use it. However, as stated in the acceptable use policies which all members of the school community sign, we expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face.

This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school or (particularly for staff) teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups.

If parents have a concern about the school, we would urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the school complaints procedure should be followed. Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset to staff, pupils and parents, also undermining staff morale and the reputation of the school (which is important for the pupils we serve).

Many social media platforms have a minimum age of 13, but the school regularly deals with issues arising on social media with pupils/students under the age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use. It is worth noting that following on from the government's Safer Internet Strategy, enforcement and age checking is likely to become more stringent over the coming years.

However, the school has to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our pupils/students to avoid or cope with issues if they arise. Online safety lessons will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse. However, children will often learn most from the models of behaviour they see and experience, which will often be from adults.

Pupils/students are not allowed* to be 'friends' with or make a friend request** to any staff, governors, volunteers and contractors or otherwise communicate via social media.

Pupils/students are discouraged from 'following' staff, governor, volunteer or contractor public accounts (e.g. following a staff member with a public Instagram account). However, we accept that this can be hard to control (but this highlights the need for staff to remain professional in their private lives). In the reverse situation, however, staff must not follow such public student accounts.

** Exceptions may be made, e.g. for pre-existing family links, but these must be approved by the Headteacher/Principal, and should be declared upon entry of the pupil or staff member to the school.*

*** Any attempt to do so may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).*

Staff are reminded that they are obliged not to bring the school or profession into disrepute and the easiest way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online. They should never discuss the school or its stakeholders on social media and be careful that their personal opinions might not be attributed to the school, trust or local authority, bringing the school into disrepute.

The serious consequences of inappropriate behaviour on social media are underlined by the fact that there have been 200 Prohibition Orders issued to teachers over the past four years related to the misuse of technology / social media.

All members of the school community are reminded that particularly in the context of social media, it is important to comply with the school policy on Digital Images and Video and permission is sought before uploading photographs, videos or any other information about other people.

Device usage

Personal devices including wearable technology and bring your own device (BYOD)

Pupils/students are not allowed to bring mobile phones into school. Any devices that are fetched into school will be confiscated by the Teacher and handed back to parents at the end of the day.

All staff who work directly with children should leave their mobile phones on silent and only use them in private staff areas during school hours. Child / staff data should never be downloaded onto a private phone.

Volunteers, contractors, governors should leave their phones in their pockets and turned off. Under no circumstances should they be used in the presence of children or to take photographs or videos. If this is required (e.g. for contractors to take photos of equipment or buildings), permission of the headteacher should be sought and this should be done in the presence of a member staff.

Parents are asked to leave their phones in their pockets and turned off when they are on site. They should ask permission before taking any photos, e.g. of displays in corridors or classrooms, and avoid capturing other children.

On trips/events away from school, teachers may use their mobile phones to contact school and in events of emergencies. Teachers must ensure that when calling parents that their numbers are switched to private.