Online Safety Policy

Date Created/Updated:	September 2023
Responsibility:	Headteacher
Date to be reviewed:	September 2024

Designated Safeguarding Lead (including Online Safety):	Will Smith, Headteacher
Online Safety Subject Leader:	Emma Blakemore
Online Safety Link Governor:	Fran Lavender/Michelle Phelan
RSHE Subject Leader:	Jess Kleeli
Network and technical support:	BlueBox IT
Data Protection Officer:	Toby Wilson

Mundella School: A school which promotes respect and healthy living
and where everyone feels valued and able to reach their full potential

Contents

1. Introduction:

Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between key school leads. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' 2023 (KCSIE), 'Teaching Online Safety in Schools' 2019 (updated 2023), statutory RSHE guidance 2019 and other statutory documents. It complements existing and forthcoming subjects including Health, Relationships and Sex Education, Citizenship and Computing; it is designed to sit alongside our school's statutory Safeguarding Policy. Any issues and concerns with online safety must follow the school's safeguarding and child protection procedures.

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department'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.

3. Policy Communication

This policy is a regularly updated document. It will be communicated to all stakeholders in the following ways:

- Posted on the school website
- Available on the internal staff network/drive
- Available in paper format in the staffroom
- 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 (especially in September refreshers)
- Clearly reflected in the Acceptable Use Policies (AUPs) for staff, volunteers, contractors, governors, pupils and 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
- AUPs are displayed in appropriate classrooms/corridors (not just in Computing corridors/classrooms)
- Reviews of this online-safety policy will include input from staff, pupils and other stakeholders, helping to ensure further engagement

4. Roles and responsibilities

4.1 The Governing Board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation. The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety.

The governors who oversee online safety is Fran Lavender & Michelle Phelan.

All governors will: Ensure that they have read and understand this policy
Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet

Key responsibilities (quotes are taken from Keeping Children Safe in Education 2023)

- Approve this policy and strategy and subsequently review its effectiveness, e.g. by asking the questions in the helpful document from the UK Council for Child Internet Safety (UKCIS) Online safety in schools and colleges: Questions from the Governing Board
- Ask about how the school has reviewed protections for **pupils in the home** and **remote-learning** procedures, rules and safeguards
- "Ensure an appropriate **senior member** of staff, from the school **leadership team**, is appointed to the role of DSL [with] **lead responsibility** for safeguarding and child protection (including online safety) [with] the appropriate status and authority [and] time, funding, training, resources and support…"
- Support the school in encouraging parents and the wider community to become engaged in online safety activities
- Have regular strategic reviews with the online-safety lead / DSL and incorporate online safety into standing discussions of safeguarding at governor meetings
- Where the online-safety curriculum coordinator is not the named DSL or deputy DSL, ensure that there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised
- Work with the DPO, DSL and headteacher 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
- Check all school staff have read Part 1 of KCSIE; SLT and all working directly with children have read Annex B; check that Annex D on Online Safety reflects practice in your school
- "Ensure that all staff undergo safeguarding and child protection training (including online safety) at induction.
- "Ensure appropriate filters and appropriate monitoring systems are in place [but…] be careful that 'over blocking' does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding". https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-standards-for-schools-and-colleges.

  School should:

  - identify and assign roles and responsibilities to manage filtering and monitoring systems.
  - review filtering and monitoring provision at least annually.
  - block harmful and inappropriate content without unreasonably impacting teaching and learning.
  - have effective monitoring strategies in place that meet their safeguarding needs.

- It also states that governing bodies and proprietors should 'review the standards and discuss with IT staff and service providers what more needs to be done to support schools and colleges in meeting this standard.

- "Ensure that children are taught about safeguarding, including online safety […] as part of providing a broad and balanced curriculum […] Consider a whole school or college approach to online safety [with] a clear policy on the use of mobile technology." NB – you may wish to refer to 'Teaching Online Safety in Schools 2019' and investigate/adopt the UKCIS cross-curricular framework 'Education for a Connected World – 2020 edition' to support a whole-school approach

4.2 The Headteacher – Will Smith

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

Key responsibilities:

- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding
- Oversee the activities of the designated safeguarding lead and ensure that the DSL responsibilities listed in the section below are being followed and fully supported
- Ensure that policies and procedures are followed by all staff
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and Sheffield Safeguarding Children Partnership.
- Liaise with the designated safeguarding lead on all online-safety issues which might arise and receive regular updates on school issues and broader policy and practice information
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO, DSL 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
- Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to child-safety first principles
- Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident
- Ensure suitable risk assessments are undertaken so the curriculum meets needs of pupils, including risk of children being radicalised
- Ensure that there is a system in place to monitor and support staff (e.g. network manager) who carry out internal technical online-safety procedures
- Ensure governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety
- Ensure the school website meets statutory requirements

4.3 The Designated Safeguarding Lead – Will Smith

The Senior Designated Safeguarding Lead (DSL) is Will Smith and the Deputy Designated Safeguarding Lead is Lisa Hewitt. The Online Safety Curriculum Lead is Emma Blakemore. The Online Safety Lead (https://www.safeguardingsheffieldchildren.org/assets/1/online_safety_coordinator_role_descriptor_sept_23.pdf) has a delegated responsibility (from the headteacher) 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, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see appendix 1) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety annually
- Checking that filtering and monitoring systems and processes are in place
- 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
- Develop and promote an Online Safety culture within the community
- To ensure that school Acceptable Use Policies are appropriate for the intended audience.
- Ensure that Online Safety is promoted to parents and carers
- Liaise with the LA, Safeguarding Sheffield Children Board and other relevant agencies as appropriate.
- To communicate regularly with school technical staff
- To ensure that the school Online safeguarding policy is systematically reviewed at agreed time intervals.
- To promote to all members of the school community the safe use of the internet and any technologies deployed within school.

This list is not intended to be exhaustive.

4.4 IT Support Services

Those with responsibility for managing the school network are responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's IT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a weekly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 1) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

4.5 All Staff and Volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet and ensuring that pupils follow the school's terms on acceptable use

- Working with the DSL to ensure that any online safety incidents are logged (see appendix 1) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Undergo online safety training which amongst other things includes an understanding of the expectations, roles and responsibilities in relation to filtering and monitoring

This list is not intended to be exhaustive

4.6 Teaching Staff

- Recognise that **RSHE** is now statutory and that it is a whole-school subject requiring the support of all staff; online safety has become core to this new subject
- 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
- 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.
- Sign and follow the staff acceptable use policy and code of conduct/handbook
- Identify opportunities to thread online safety through all school activities as part of a whole school approach in line with the RSHE curriculum, 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 in school or for homework or remote teaching, encourage and talk about appropriate behaviour and how to get help and consider potential risks and the age-appropriateness of websites (find out what appropriate filtering and monitoring systems are in place)
- When supporting pupils remotely, be mindful of additional safeguarding considerations – refer to the remotesafe.lgfl.net infographic which applies to all online learning.
- Carefully supervise and guide pupils when engaged in learning activities involving online technology, supporting them with search skills, critical thinking, age appropriate materials and signposting, and legal issues such as copyright and GDPR.
- Be aware of security best-practice at all times, including password hygiene and phishing strategies.
- Prepare and check all online source and resources before using
- Encourage pupils/students to follow their acceptable use policy at home as well as at school, remind them about it and enforce school sanctions.
- Notify the DSL/OSL of new trends and issues before they become a problem
- Take a zero-tolerance approach to bullying and sexual harassment (your DSL will disseminate relevant information from the updated 2021 DfE document on this)
- Read UKCIS Sharing Nudes and Semi –Nudes: How to Respond to an Incident.
- Be aware that you are often most likely to see or overhear online-safety issues (particularly relating to bullying and sexual harassment and violence) in the playground, corridors, toilets and other communal areas outside the classroom – let the DSL/OSL know
- Receive regular updates from the DSL/OSL and have a healthy curiosity for online safeguarding issues
- Model safe, responsible and professional behaviours in their 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.

4.7 RSHE Lead – Jess Kleeli

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSHE / Relationships education, relationships and sex education (RSE) and health education curriculum. "This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers will address online safety and appropriate behaviour in an age appropriate way that is relevant to their pupils' lives."
- This will complement the computing curriculum, which covers the principles of online safety at all key stages, with progression in the content to reflect the different and escalating risks that pupils face. This includes how to use technology safely, responsibly, respectfully and securely, and where to go for help and support when they have concerns about content or contact on the internet or other online technologies.
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE / RSHE.
- Note that an RSHE policy should now be included on the school website.
- Work closely with the Computing subject leader to avoid overlap but ensure a complementary whole-school approach, and with all other lead staff to embed the same whole-school approach

4.8 Computing Lead – Emma Blakemore

Key responsibilities:

- Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum
- Work closely with the RSHE lead to avoid overlap but ensure a complementary whole-school approach
- Work closely with the DSL/OSL 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

4.9 Parents and Carers

Parents are expected to:

Notify a member of staff or the headteacher of any concerns or queries regarding this policy Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

What are the issues? - UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parentsand-carers/what-are-issues
Hot topics - Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

Key responsibilities:

- Read, understand, sign and adhere to the student/pupil acceptable use policy and review this annually
- Avoid any private communication or use of personal logins/systems to communicate with or arrange meetings with school staff or tutors
- Understand the importance of reporting abuse, misuse or access to inappropriate materials, including any concerns about a member of school staff or supply teacher or online tutor
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology, at school, home or anywhere else.
- To understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of school and realise that the school's acceptable use policies cover actions out of school, including on social media
- Remember the rules on the misuse of school technology – devices and logins used at home should be used just like if they were in full view of a teacher.
- Understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at school or outside school if there are problems
- If organising private online tuition, remain in the room if possible, ensure the child knows tutors should not arrange new sessions directly with the child or attempt to communicate privately. Further advice available in the Online Tutors – Guidance for Parents and Carers poster at parentsafe.lgfl.net, which is a dedicated parent portal offering updated advice and resources to help parents keep children safe online

4.10 Visitors and Members of the Community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

5. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum.

In Key Stage 1, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in Key Stage 2 will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

The safe use of social media and the internet will also be covered in other subjects where relevant.

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this. Children will be made aware of the NSPCC helpline and school's internal reporting channels.

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

Content: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

Contact: being subjected to harmful online interaction with other users; for example: child to child 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; for example, 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).

Commerce - risks such as online gambling, inappropriate advertising, phishing and or financial scams.

Online Safety is taught through a combination of discrete lessons and when appropriate throughout the curriculum. Discrete online safety lessons are identified within our RSHE and PHSE lessons and the policy for RSHE and PHSE can be read in conjunction with this one. The school will report any potential risks and will ensure that online safety is considered consistently through planning the curriculum, staff training, the work of the designated safeguarding lead and parental engagement. The school has a specific policy for remote learning provision.

6. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents. If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL. Concerns or queries about this policy can be raised with any member of staff or the headteacher.

7. Cyber-bullying

7.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

7.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their groups, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyberbullying. This includes RSHE and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL and Online Safety Lead will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

7.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

Cause harm, and/or
Disrupt teaching, and/or
Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

Delete that material, or
Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

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

8. Acceptable use of the internet in school

All pupils, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role. Websites will be monitored that are visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

9. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them during the school day. This includes:

- Lessons
- Clubs before or after school, or any other activities organised by the school

Children will hand in their mobile phone to the class teacher each morning where they will be stored securely throughout the school day.

10. Staff using work devices outside school

Work devices must be used solely for work activities. Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the Online Safety Lead.

11. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

12. Handling online safety concerns and incidents

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/RSHE and Citizenship).
General concerns must be handled in the same way as any other safeguarding concern; stakeholders should err on the side of talking 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
- Anti-Bullying Policy
- Behaviour Policy (including school sanctions)
- Acceptable Use Policies
- Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc)

13. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings). The DSL and deputy will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

14. Monitoring arrangements

The Online Safety Lead will log behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 1.

This policy will be reviewed annually by the Online Safety Lead together with the DSL. At every review, the policy will be shared with the governing board.

15. Links with other policies

This online safety policy is linked to our:

Safeguarding policy
Behaviour policy
Staff disciplinary procedures
GDPR Data Protection Policy
Complaints procedure

Appendix 1 – Online Safety Note of Concern

Concerns can be logged directly onto CPOMS or complete the form below

Note of Concern			
Child's Name :			
Child's DOB :			
Male/Female :	Class:	Disability Y/N :	Age:
Date and time of concern/incident :			
Nature of concern : Physical □ Emotional □ Disclosure made by child □ Other □			
Details of concern : Differentiate between fact, allegation, observation and opinion. Describe in sufficient detail. Use child's own words. Include body map (if relevant) to show any visible injuries.			
Your response : (what did you do/say following the concern)			
Your name :	Date: Time:		
Form received by: STL/DSD/DSL	Date and time of receipt:		
Form scanned to CPOMS: Yes/No			

Action and response of DSD/DSL

Action	By who	Date & time

Feedback given to member of staff reporting concern Y/N	Information shared with any other staff Y/N

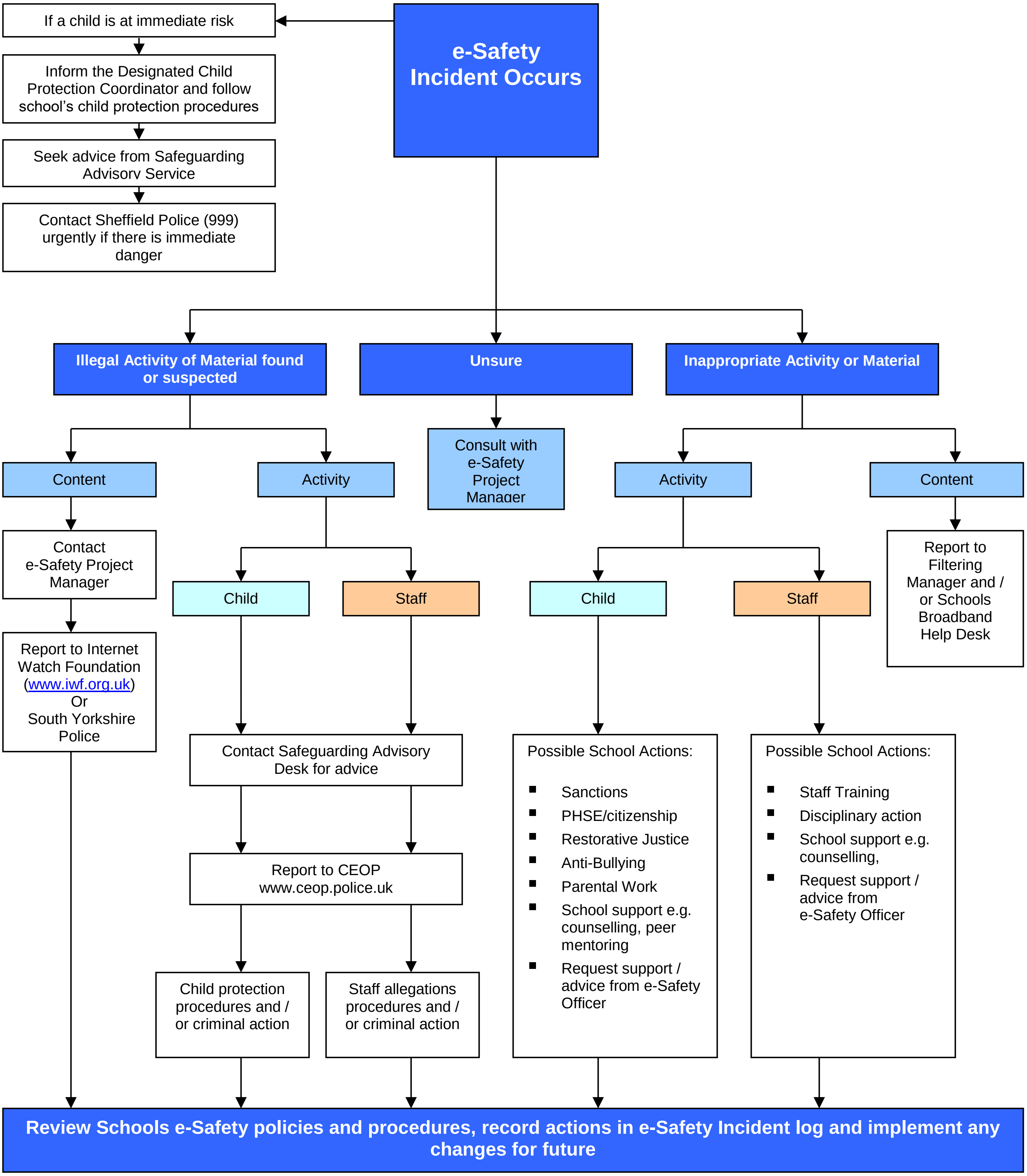
Name: ………………………………………………………………… Position held…………………………………………………………

Date:

Appendix 2 - Response to an Incident of Concern

Contacts

- Sheffield Safeguarding Advisory Desk 0114 205 3535
- e-Safety Project Manager
- Julia Codman 0114 293 6945
- Sheffield Police 0114 220 2020
- Child Exploitation and Online Protection Centre (CEOP) www.ceop.police.uk



e-Safety Incident Occurs

If a child is at immediate risk

Inform the Designated Child Protection Coordinator and follow school's child protection procedures

Seek advice from Safeguarding Advisorv Service

Contact Sheffield Police (999) urgently if there is immediate danger

Illegal Activity of Material found or suspected

Unsure

Inappropriate Activity or Material

Content

Contact e-Safety Project Manager

Report to Internet Watch Foundation (www.iwf.org.uk) Or South Yorkshire Police

Activity

Child

Staff

Contact Safeguarding Advisory Desk for advice

Report to CEOP www.ceop.police.uk

Child protection procedures and / or criminal action

Staff allegations procedures and / or criminal action

Consult with e-Safety Project Manaqer

Activity

Child

Staff

Possible School Actions:

- Sanctions
- PHSE/citizenship
- Restorative Justice
- Anti-Bullying
- Parental Work
- School support e.g. counselling, peer mentoring
- Request support / advice from e-Safety Officer

Possible School Actions:

- Staff Training
- Disciplinary action
- School support e.g. counselling,
- Request support / advice from e-Safety Officer

Content

Report to Filtering Manager and / or Schools Broadband Help Desk

Review Schools e-Safety policies and procedures, record actions in e-Safety Incident log and implement any changes for future