Abbey Lane Primary School

Online Safety Policy

Reviewed April 2023

Online Safety Policy

Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between key school leads. Online Safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

This policy is designed to sit alongside the school's statutory Safeguarding Policy and will operate in conjunction with additional policies, including those for Behaviour, Anti-Bullying, Curriculum (RHE and Computing) and Data Protection.

This policy aims to:

- Help all stakeholders to recognise that online/digital behaviour standards (including social media activity) should be upheld beyond the confines of the school gates and school day, and regardless of device or platform.
- Facilitate the safe, responsible, respectful and positive use of technology to support teaching and learning, increase attainment and prepare children for the risks and opportunities for today's and tomorrow's digital world, to survive and thrive online.
- Help school staff, including volunteers and Governors, to understand their roles and responsibilities to work safely and responsibly with technology.
- Establish clear structures and procedures for dealing with and recording online safety concerns, in line with how any safeguarding incidents are dealt with in the school.

Contents

School Online Safety Policy

The school will appoint an Online Safety lead. This will be a member of the Senior Leadership Team (SLT). All staff will receive appropriate and regular Online Safety training.

The Online Safety Policy has been written by the school, building on the Sheffield Children and Young Peoples' Directorate and Government guidance. It has been agreed by (SLT) and seen by governors.

The Online Safety Policy will be reviewed annually. This policy will next be reviewed April 2024.

Why is internet use important?

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 school's management information and administration systems.

Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality Internet access.

Pupils will use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security, including when using Google Classroom.

How does internet use benefit education?

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- educational and cultural exchanges between pupils world-wide;
- 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;
- exchange of curriculum and administration data with the Local Authority and DfE;
- access to learning wherever and whenever convenient.

How can internet use enhance learning?

- The school Internet access will be designed expressly for pupil use and includes filtering appropriate to the age of pupils.

- The school recognises and addresses the 4 key categories of risk, to enhance learning through a broad and balanced curriculum.

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access will be planned in to the Computing and other schemes of work, to enrich and extend learning activities.
- Staff will guide pupils in online activities that will support learning outcomes, planned for the pupils' age and maturity.
- Pupils will be educated in the effective and safe use of the Internet, including the skills of knowledge location, retrieval and the evaluation of search outcomes.
- Pupils will be educated in the effective development of positive online relationships through the RHE curriculum.
- All children will have access to their Google Classroom, which may be utilised in school or at home, to promote learning and to help with isolation issues related to COVID19.
- All staff will identify opportunities to thread Online Safety through all school activities, both outside the classroom and within the curriculum and make the most of unexpected learning opportunities as they arise.

Impact of teaching and learning

School ensures that all children receive a broad and balanced Online Safety curriculum, using the Sheffield Online Safety scheme of work. This is delivered through the Computing and RHE curriculums, and at every other appropriate opportunity in school.

We know that our curriculum is having an impact because:

- Children can talk with confidence about Online Safety, articulating ideas using a rich, developing vocabulary.

- Children can question and reflect on ideas during and following lessons and because of this, children are able to offer support to their peers.
- Children know how/who to report Online Safety concerns to.

Authorised Internet Access

- The school will maintain a current record of all staff and pupils who are granted Internet access.
- All staff must read and sign the 'Staff Information Systems Code of Conduct' before using any school ICT resource.
- Parents will be informed that pupils will be provided with supervised Internet access.
- Parents will be asked to sign and return a consent form for pupil access.
- Children will sign an age appropriate Acceptable Usage Policy (AUP) referring to responsible computer, tablet and internet use.

World Wide Web

- If staff or pupils discover unsuitable sites, the URL (address), time and content will be reported to the Local Authority helpdesk via the Online Safety coordinator or network manager (technician).
- School will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.
- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

Email

- Whole class or group email addresses are used in school, if applicable to Computing units of work.
- Personal pupil email addresses, set up by school, are used to access Google Classroom, in school and at home.
- Pupils must immediately tell a teacher if they receive offensive email.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission.
- Access in school to external personal email accounts may be blocked.
- Email sent to external organisations or parents/carers should be written carefully and authorised before sending, in the same way as a letter written on school headed paper and must comply with GDPR rules (first names only).
- The forwarding of chain letters is not permitted.
- Most electronic communication with parents will be made using school email. Some will be done on Google Classroom.
- A new thread must be started for all email communication.

Social Networking

- Schools should block/filter access to social networking sites and newsgroups unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils should be advised not to place personal photos on any social network space.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others.

Filtering and Monitoring

The school will work in partnership with the Local Authority and the Internet Service Provider to ensure filtering systems are as effective as possible.

Abbey Lane uses educational broadband connectivity through Virgin. The school will do all it reasonably can to limit children's exposure to online risks through school provided IT systems/devices and will ensure that appropriate filtering and monitoring systems are in place. The school's governors and leaders have ensured that our school has age and ability appropriate filtering and monitoring in place to limit learner's exposure to online risks. The school is aware of the need to prevent 'over blocking' as that may unreasonably restrict what children can be taught with regards to online activities. Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from the leadership team. The leadership team will also ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate. Abbey Lane uses Smoothwall which blocks sites that are categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature.

The school filtering system blocks all sites on the Internet Watch Foundation (IWF) list and blocks access to illegal Child Abuse Images and Content (CAIC).

Abbey Lane has a clear procedure for reporting filtering breaches.

- If pupils discover unsuitable sites, they will be required to report the concern immediately to a member of staff.
- The member of staff will report the concern (including the URL of the site, if possible) to the Designated Safeguarding Lead and/or Online Safety Lead.
- The breach will be recorded and escalated as appropriate.
- Parents/carers may be informed of filtering breaches involving their child.
- Any material that the school believes is illegal will be reported immediately to the appropriate agencies, such as: IWF, South Yorkshire Police or CEOP.

There are three types of appropriate monitoring identified by the Safer Internet Centre that work together. These are:

1. Physical monitoring (adult supervision in the classroom, at all times)

2. Internet and web access monitoring
3. Active/Pro-active technology monitoring services

At Abbey Lane, we have decided that, for no. 3, Smoothwall is the appropriate service because it monitors the internal network for both pupils and staff.

Online Video Conferencing Platforms (Zoom & Microsoft Teams)

- Children will only ever use these platforms in school (we do not currently conduct 'live' learning sessions between school and home as a result of COVID 19).
- Children will always be supervised by a member of school staff, when using these platforms.
- Children will only use these platforms in school following parental consent.

Managing Emerging Technologies and Mobile Phones

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will not be used for personal use during lessons or formal school time. The sending of abusive or inappropriate messages is forbidden.
- Staff will be issued with a school phone where contact with pupils or parents/carers is required, e.g. on a school trip or visit. Teachers using their own mobile phone in an emergency will ensure that the number is hidden to avoid parents or children accessing a teacher's private phone number.
- Child/staff data should not be downloaded on to a private phone.
- For more detail, please see the school's *Use of Mobile Phones Policy.*

Home Devices

- Home devices may be issued to some children who are working remotely on Google Classroom. In these cases, parents will be asked to sign a Device Loan Agreement for Pupils.
- These are restricted to the apps/software installed by the school and are intended for school learning only (all usage may be tracked).

Published Content and the School Website

- The contact details on the website should be the school address, email and telephone number. Staff or pupils personal information will not be published.
- The headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing Pupils' Images and Work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified by name.

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website or Google Classroom.
- Pupils' full names will not be used anywhere on the website or Google Classroom, particularly in association with photographs.
- Work can only be published with the permission of the pupil and parents.

Information System Security

- School IT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the Local Authority.

Protecting Personal Data

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

Assessing Risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Sheffield City Council can accept liability for the material accessed, or any consequences of internet access.
- The school should audit IT use to establish if the Online Safety policy is adequate and that the implementation of the Online Safety policy is appropriate.

Handling Online Safety Complaints

- Safeguarding is the responsibility of all staff. Any issues or concerns with Online Safety involving children, will be dealt with following the school's safeguarding and child protection procedures.
- Complaints of internet misuse will be dealt with by a senior member of staff and the Online Safety lead.
- Any complaint about staff misuse must be referred to the headteacher.
- The school commits to take all reasonable precautions to ensure online safety, but recognises that incidents will occur both inside school and outside of school; and that those from outside school will continue to impact pupils when they come into school or during extended periods away from school. All members of the school community are encouraged to report issues swiftly to allow school to deal with them quickly and sensitively through the school's safeguarding processes.
- Pupils and parents will be informed of how a concern can be raised in school.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

Communication of Policy

Pupils

- Age appropriate Acceptable Usage Policies will be displayed in all classrooms.
- Pupils will be informed that internet use will be monitored.

Staff

- All staff will be given the School Online Safety Policy and its importance explained.
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Parents

- Parents' attention will be drawn to the School Online Safety Policy, which includes pupil Acceptable Usage Policies and the complaints procedure, via the school prospectus and on the school website.

Appendix A – Flowchart for responding to Online Safety incidents in school

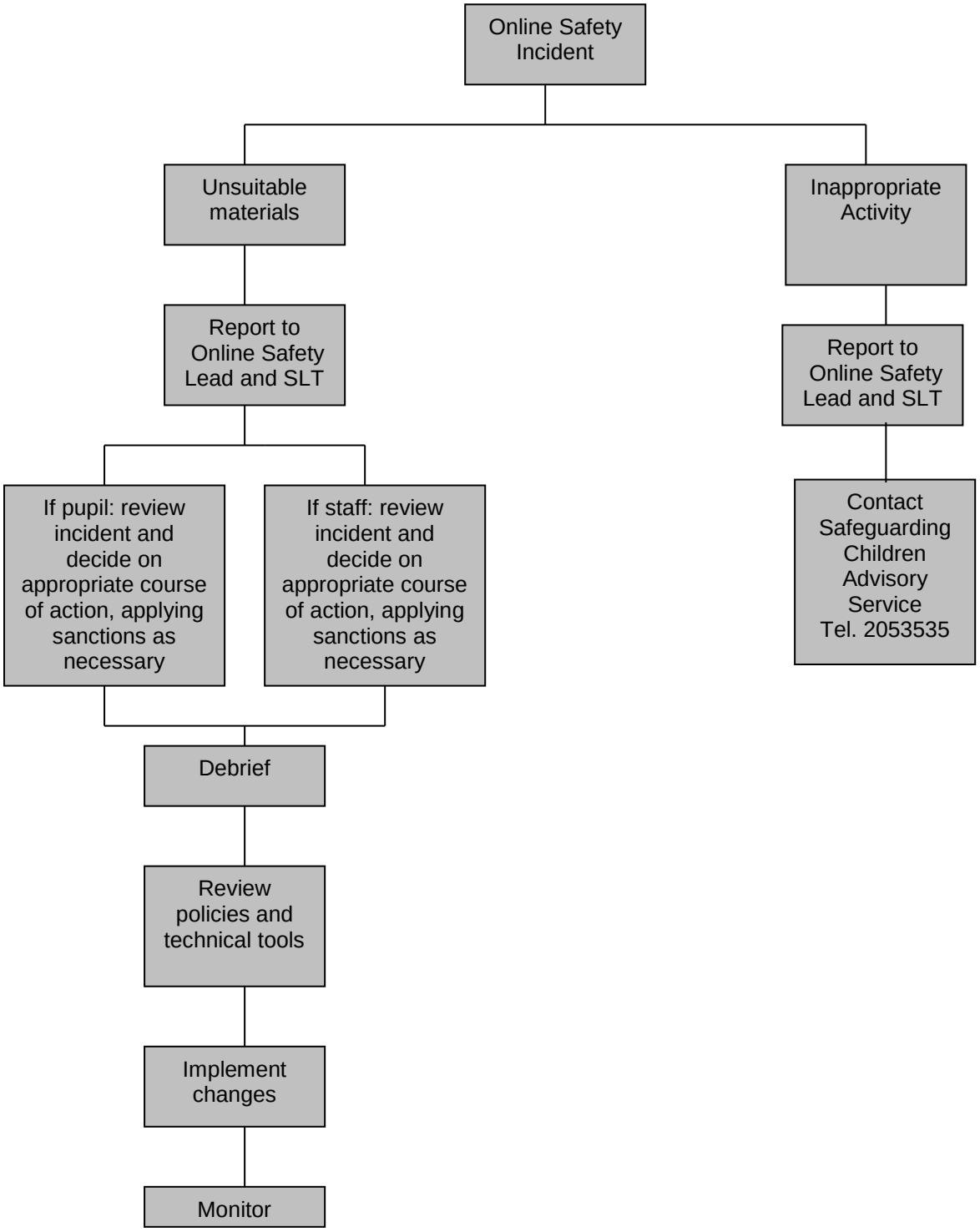
Appendix B - Age appropriate Acceptable Usage Policies for children

Appendix C - Staff Acceptable Use Policy

Appendix D - Abbey Lane Primary School Online safety incident report form

Appendix A

Flowchart for responding to Online Safety incidents in school



Appendix B
Key Stage 1

Think before you click

S 

I will only use the Internet and email with an adult or with adult permission.

A 

I will only click on icons and links when I know they are safe.

F 

I will only send friendly and polite messages.

E 

If I see something I don't like on a screen, I will always tell an adult.

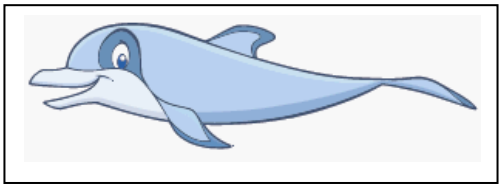
I promise to keep to these rules:

Abbey Lane Primary School LKS2 Acceptable Use Policy

This is how we stay safe and look after school equipment when we use computers:

Staying Safe

- I will ask *a teacher / an adult* if I want to use the computer/IPad (in school and at home).
- I will only use activities that *the teacher /an adult* has told or allowed me to use.
- I will click on 'Hector' and tell *the teacher / an adult* if I see something that upsets me on the screen.



- I will not share any usernames and passwords with anyone or try to use another person's username and password.
- I will not share personal information about myself or others when I am online.

Respecting other people and school equipment

- I will only say friendly, polite things online.
- I will take care of the computer/IPad and other equipment.
- I will ask for help from *the teacher / an adult* if I am not sure what to do or if I think I have done something wrong.

I know that if I break the rules I might not be allowed to use a computer or IPad.
I have read and understood the rules for using computers/IPad and the internet.
Signed by:

Upper Key Stage 2

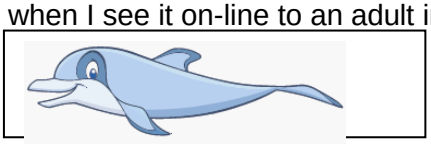
Abbey Lane Primary School UKS2 Acceptable Use Policy

This Acceptable Use Policy is intended to ensure that we stay safe and look after school equipment when we use the internet and other communication technologies.

The school will try to ensure that you will have good access to ICT to enhance your learning and will, in return, expect you to agree to be responsible users.

For my own personal safety:

- I understand that the school will monitor my use of computers and other digital communications.
- I will not share our class' usernames and passwords with anyone or try to use another class' username and password.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line.
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line to an adult in school or to my parents (click on 'Hector' in school).



I understand that everyone has equal rights to use technology to support our education:

- I understand that the school computer systems are for educational use and that I will not use them for personal or recreational use unless I have permission to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or change any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or share images of anyone without their permission.

I understand that the school has a responsibility to keep the technology secure and safe:

- I will not use my mobile phone whilst on school grounds. I will only use personal devices, such as USB devices etc, if I have permission from an adult.
- I understand the risks and will not try to upload, download or access any materials which may cause harm or distress to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any attachments to emails, unless I know and trust the person who sent the email, due to the risk of the attachment containing viruses or other harmful programmes.

- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.
- I will not use chat and social networking sites because I am not old enough.

When using the internet for research for my school work, I understand that:

- When I am using the internet to find information, I should take care to check that the information that I find is accurate (I will not believe everything that I read), as I understand that the work of others may not be correct.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school could take action against me if I am involved in incidents or inappropriate behaviour that are included in this agreement, when I am out of school as well as in school. Examples of this are cyberbullying, sending/receiving inappropriate images and misuse of personal information.
- I understand that if I do not follow this Acceptable Use Policy Agreement, it will lead to disciplinary action by the school and that my parents will be contacted.

I have read and understand the above and agree to follow these guidelines when:

- I use the school computers and equipment.
- I use my own equipment in school (when allowed) eg USB devices (not mobile phones).
- I use my own equipment out of school in a way that is related to me being a member of this school eg communicating with other members of the school e.g. through, mobile phones, accessing school email, Learning Platform (Google Classroom), website etc.

Signed by:

Appendix C

Staff Information Systems Code of Conduct

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's Online Safety policy for further information and clarification.

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional rôle.
- I understand that school information systems may not be used for private purposes, without specific permission from the headteacher.
- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the school Online Safety Coordinator or the Designated Child Protection Coordinator.
- I will ensure that any electronic communications with pupils are compatible with my professional role. I will ensure that I do not use an internet messaging service which has any relation to Abbey Lane or pupils.
- I will promote Online Safety with pupils in my care and will help them to develop a responsible attitude to system use and to the content they access or create.
- I will use professional discretion when accessing social networking sites including facebook, twitter, whats app etc. I am aware that such sites are part of the public domain, so care must be taken if I choose to access these, that there is nothing that could bring myself, other stakeholders or the school into disrepute.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and agree with the Information Systems Code of Conduct.

Signed: …… Capitals: …… Date: ……

Appendix D

Abbey Lane Primary School Online safety incident report form

Details of incident

Date happened:

Time:

Name of person reporting incident:

If not reported, how was the incident identified?

Where did the incident occur?
☐ In school ☐ Outside school

Who was involved in the incident?
☐ child/young person ☐ staff member ☐ other (please specify

Type of incident:
☐ bullying or harassment (cyber bullying)
☐ deliberately bypassing security or access
☐ hacking or virus propagation
☐ racist, sexist, homophobic, transphobic, bi-phobic, religious hate material
☐ terrorist material
☐ online sexual grooming
☐ online radicalisation
☐ child abuse images
☐ on-line gambling
☐ soft core pornographic material
☐ illegal hard core pornographic material
☐ other (please specify)

Description of incident

Nature of incident

☐ **Deliberate access** Did the incident involve material being; ☐ created ☐ viewed ☐ printed ☐ shown to others ☐ transmitted to others ☐ distributed Could the incident be considered as; ☐ harassment ☐ grooming ☐ cyber bullying ☐ breach of AUP ☐ **Accidental access** Did the incident involve material being; ☐ created ☐ viewed ☐ printed ☐ shown to others ☐ transmitted to others ☐ distributed

Action taken

Staff	**Child/Young person**
☐ Incident reported to headteacher/SLT ☐ Advice sought from LADO ☐ Referral made to LADO ☐ Incident reported to police ☐ Incident reported to IT ☐ Disciplinary action to be taken ☐ Online Safety policy to be reviewed/amended	☐ incident reported to Headteacher/SLT ☐ advice sought from Safeguarding/Social Care ☐ referral made to safeguarding/Social Care ☐ incident reported to police ☐ incident reported to social networking site ☐ incident reported to IT ☐ child's parents informed ☐ child/young person debriefed ☐ Online Safety policy to be reviewed/amended

Outcome of incident/investigation

Signed: Date:

Name of person receiving the form (Online Safety Lead/SLT):

Date received: Time received: