Irby Primary School

Inspiring Pupils Successfully

Irby Primary School

E-Safety Policy

September 2023

IRBY PRIMARY SCHOOL E-SAFETY POLICY

Irby Primary School has appointed the Headteacher, Mr R Dixon as the ESafety Co-ordinator in addition to his role as Designated Safeguarding Lead.

Our E-Safety Policy has been written taking into account current Government advice.

The E-safety Policy will be reviewed annually and will be next reviewed in September 2024.

Why is Internet use important?

The purpose of Internet use in school is to raise educational standards, to promote student 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.

How does Internet use benefit education?

Benefits of using the Internet in education include:

- Access to learning wherever and whenever convenient.
- 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 DCSF.

How Can Internet Use Enhance Learning?

- The school Internet access will be designed expressly for student use and includes filtering appropriate to the age of pupils.
- 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 to enrich and extend learning activities.

- Staff should guide pupils in on-line activities that will support learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

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 'Acceptable ICT Use Agreement' before using any school ICT resource during induction.
- 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 student access when logging in for the first time.
- Pupils must apply for Internet access individually by agreeing to comply with the Responsible Internet Use statement.

World Wide Web

- If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to Headteacher and recorded in the eSafety log.
- 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

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication or arrange to meet anyone without specific permission.
- Access in school to external personal e-mail accounts may be blocked.
- E-mails sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

Password Protection

- School issues passwords.
- Staff & pupils encouraged to change their passwords on a regular basis.
- No use of generic passwords.
- Pupils must not disclose passwords to other pupils.

Social Networking

- Access to social networking sites and newsgroups are blocked/filtered via the Wirral Intranet.
- 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 (Social Media Parental Agreement).

Filtering and Monitoring

- Irby Primary School will work in partnership with the Wirral IT Services (and has in place a Service Level Agreement) to ensure filtering systems are as effective as possible.
- The Authority regularly receives a file update to ensure the firewall remains up to date with all new recognized threats and/or inappropriate sites thus ensuring they are inaccessible on the school network and any devices.
- An annual review of Filtering and Monitoring standards and responsibilities will take place annually in September with reports provided on a monthly basis and in the event of a filtering incident.
- The DSL, Mr R Dixon, is the named person responsible for meeting the filtering and monitoring standard as set out in the document: Meeting digital and technology standards in schools and colleges.
- A Filtering Review document will be completed and shared with Governors on an annual basis.

Prevent

- At Irby Primary, we must ensure that children are safe from terrorist and extremist material when accessing the internet in school and we therefore ensure that suitable filtering is in place. It is also important that we teach pupils about online safety generally.
- The balance between educating pupils to take a responsible approach and the use of regulation and technical solutions continues to be judged carefully.

Video Conferencing

- Pupils should ask permission from the supervising teacher before making or answering a videoconference call
- Videoconferencing will be appropriately supervised for the pupils' age.

USB memory sticks & other Portable Data Storage Devices

- Staff to consider what data should be stored on USB sticks/other data storage devices.
- Sensitive data should be encrypted.
- Staff must not store files with sensitive information on their home computers.

Clouds

- Images and videos of children must not be saved on personal clouds.

- Staff must make sure that personal devices (e.g. mobile phones and personal computers) outside of school are not left unprotected without a password to ensure that no third party can access school emails or other documents (e.g. Google or shared drive).

Digital Cameras and Tablets

- Staff to use school cameras or school ipads/tablets to photograph pupils or record images of children's work and of special events.
- Photographs will not be published on newsletters, websites, Twitter or other media will not be published without the consent of the children's parent.
- Staff will not download any images to personal computers.
- Staff must not use personal equipment to photograph pupils.
- Storage cards to be cleared when the camera is returned.

Storage of Photographs

- Photographs to be stored in secure area within school network.
- Photographs to remain on school premises (when practicable, e.g. off site school trips, with images only to be downloaded to school network).
- Photographs to be deleted when no longer required.
- Current LA policy is adhered to regarding photographing & publishing images of children.

Mobile Phones & Other Hand Held/Communication devices

- Mobile phones & other hand held communication devices should not be used for personal use in the lesson or formal school time (pupils & staff).
- Pupils who need a mobile phone in school for safety reasons must hand them into their member of staff and they must be locked away until the end of the day.
- Mobile Phone – Bluetooth should be turned off.
- Sending of abusive or inappropriate messages is forbidden.
- Staff/volunteers and visitors are not to use their mobile phones unless in the staffroom or the front car park.

Mobile Data and Smart Watches

- Children will not use cellular data (e.g. 3G, 4g and 5G) to connect to any school devices.
- All internet connections will be through the school Wi-Fi so that the school filter is active.
- Watches (e.g. smart watches) that use the internet to receive messages (text, email and calls) play games. Record photographs or sound or make calls are not permitted to be brought to school by children.
- Staff must not use personal smart watches to access these features when working with children.

Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out by the safeguarding officer and agreed by the governing body, before use in school is allowed.

- Mobile phones/ handheld communications devices/ gaming consoles will not be used for personal use during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

Published Content and the School Web Site

- The contact details on the Web site will be the school address, e-mail and telephone number. Staff or pupils personal information will not be published
- The Headteacher 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 be appropriate for the context.
- Pupils' full names will not be used anywhere on the website, post or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained annually before photographs of pupils are published on the school Web site or VLE
- Work can only be published with the permission of the student and parents

Information System Security

- School ICT 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.
- Also reference the use of 'USB memory sticks and other portable storage devices' section.

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Assessing Risks

- Irby Primary 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 Wirral Metropolitan Borough Council can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT use to establish if the eSafety policy is adequate and that the implementation of the eSafety policy is appropriate every 12 months.

Handling E-Safety Complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff, Safeguarding officer or Headteacher.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection and safeguarding procedures.

- Pupils and parents will be informed of the complaints procedure.

Communication of Policy

Pupils

- Rules for Internet access will be posted in all networked rooms.
- Pupils will be informed that internet use will be monitored.
- Children learn through tailored units of work in Computing how to keep themselves safe online and how to ask for help when required.

Staff

- All staff will be given the school's E-safety Policy and its importance explained.
- Staff should be aware that internet traffic can be monitored and traced to individual use. Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues

Governors

- Policies reviewed and approved through the appropriate committee meetings and Governors to be involved in the monitoring of the policies implementation and effectiveness.

Parents

- Parents' attention will be drawn to the school's E-Safety Policy in newsletters and on the school website.

Visitors

- Visitors to school will be informed about the E-Safety Policy at the reception desk.
- Rules for visitors clearly displayed and given in the Visitor Policy (i.e. use of mobile phone etc).

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 E-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 role.
- 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 ESafety Coordinator or the Designated Child Protection Coordinator.
- I will ensure that any electronic communications with pupils are compatible with my professional role.
- I will promote ESafety 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.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of email 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: …… Printed: …… Date: ……

Accepted for school: ……. Capitals: ……..…

INTERNET AND SOCIAL MEDIA

RESPONSIBLE USE OF THE INTERNET: Computing is a major part of the curriculum and Irby Primary School provides monitored access to the Internet. Pupils will be able to research information from museums, libraries, news providers and suitable web sites as part of their programme of learning. We are mindful of concerns regarding pupils having access to undesirable materials, and take positive steps to minimise that possibility. Our Internet provider operates a multi-level filtering system which restricts access to inappropriate material. All our screens are in public view and as stated above, access will be monitored. Pupils are also taught to report anything which they feel is inappropriate. The school will also teach the importance of respectful communication on any device and how to stay safe when online.

Please find enclosed a copy of the Rules for Responsible Computer Internet Use that we are operating, please explain these rules to your child.

PARENTS/CARERS

TWITTER: On our Twitter account we will celebrate achievements with photographs and videos of work and pupils. On this platform we will usually refer to children by class or group name i.e. Green Class or the Irby Football Team; however, we may use first names only occasionally, again with your permission if given below, to acknowledge and celebrate individuals' involvement or effort. If you have a reason for your child's image not to be displayed on our Website or Twitter feed, please indicate below so that we can update our records.

EVENTS: Occasionally we are involved in events, visits or initiatives whereby the press request photographs. Again if you have any reason for your child's photo/name not to appear in the press, please indicate below.

TEMPEST PHOTOGRAPHY: Every year a photographer takes a class photo of the children and in order that parents can view before purchase, they are displayed in the reception area and then remain throughout the year. We also display photographs from productions and other events. Again, if you have a reason for your child's image not to be displayed in reception, please indicate below.

PERFORMANCES: During your child's time at school he/she will take part in various assemblies and school productions/events. As parents ourselves, we understand the importance of taking photos and film in order to capture memories. However, we take the safeguarding of all children very seriously. In light of this, we ask that during any school event you only focus on your own child and we ask that you will sign the consent slip below agreeing that you or members of your **family/friends**, will **not** reproduce any images publicly or use them in social media, including Whatsapp.

RULES FOR RESPONSIBLE COMPUTER USE

Irby's Digital Leaders are redesigning posters for online safety rules (Sept 2021).

These rules will keep you safe and help us be fair to others when using I Pads, Chromebooks, electronic devices, computers and the internet at school.
I agree that:

- I will only access the system through the correct log-in procedure and will keep any passwords secret. I will not share any passwords (e.g. Purple Mash or Mathletics).
- I will not open or delete other people's files.
- I will stick to the task which I have been asked to do.
- I will not bring CDs, memory sticks or other storage devices from outside school unless I have been given permission by my teacher.
- I will make sure that all electronic contact with others is responsible, polite and sensible (from home and school).
- I will ask permission from a member of staff before using the Internet.
- I will not give my name, home address or telephone number, or arrange to meet someone (from school or home).
- I will report any unpleasant material or comments encountered at school or at home to my teacher or parent or carer. I understand this report would be confidential and would help protect other pupils and myself.
- I understand that the school will check my computer files and may monitor the Internet sites I visit. I know that my parent/carer will be contacted if school staff are concerned about my e-safety.
- I will not name myself or any other pupils when online.

- I will not take photos/videos of other pupils unless they have parental permission for their image to appear on the internet.

- I will not link images with any user IDs.

INTERNET AND SOCIAL MEDIA CONFIRMATION AND CONSENT

I have explained the computer rules to my child. ___

I accept that the school will do everything within its power to prevent my child from accessing materials that are unacceptable. I also accept my responsibility for making it clear to my son/daughter that he/she must follow the school's instructions and guidance, and that he/she will report any questionable material they encounter to the teacher immediately who will pass on the information to the Computing Subject Leader.

Tick one

I give permission for my child's image/video to appear on the school Twitter feed.
I **do not** give permission for my child's image/video to appear on the school Twitter feed

---

Tick one

I give permission for my child's first name only to appear on the school Twitter feed
I **do not** give permission for my child's first name only to appear on the school Twitter feed

---

Tick one

I give permission for my child's image/video to appear on the school website
I **do not** give permission for my child's image/video to appear on the school website

---

Tick one

I give permission for my child's image/video to appear in the press/press media
_____
I **do not** give permission for my child's image/video to appear in the press/press media

---

Tick one

I give permission for my child's first name only to be printed in the press
I **do not** give permission for my child's first name to be printed in the press

---

Tick one

I give permission for my child's class photograph to be displayed in the reception area
I **do not** give permission for my child's class photograph to be displayed in the reception area

I understand that if I take any photos or film at any school event that I must only focus on my own child/children. I also agree not to reproduce any images publicly or use them in social media, including Whatsapp.

CHILD'S NAME_____ DATE:_____

PARENT/CARER NAME_____PARENT/CARER SIGNATURE: _____

TAPESTRY - ONLINE LEARNING JOURNAL

We use Tapestry as our online learning journal provider. We will use this to send you observations of your child which might include photographs and videos. If you give your consent below, you will be able to see group observations, which might include photos and videos with other children in and consequently, other parents might be able to view photos and videos of your child. You can view, like and comment on the observations we make for your child. You can also add your own observations of what your child does outside of the setting.

If you give your consent, we will set you up with your own account using your email address. This account will be directly linked to your child's account, which means you will only be able to see observations that include your child. You will then be able to login with your email address and password to either the browser version of Tapestry (tapestryjournal.com) or to the app.

Please see the instructions within the pack. If you choose to use the app, after you login initially, you can use a 4-digit PIN to quickly log back in.

Tapestry securely stores all the data we input to our account on their servers. If you want to find out more information about how Tapestry keeps our data safe and secure, you just need to go to https://tapestry.info/security.html. Please complete the slip below to provide your consent.

Please note, you can withdraw your consent, in writing, or request to see photos taken at any time. This form is valid for the duration of your child's time at Irby Primary School. It is your responsibility to let us know if you want to withdraw or change your consent at any time

---

TAPESTRY CONSENT

I give permission for a Tapestry account to be created for my child: Y / N

The e-mail address I would like to link with the account is:

I give consent for my **child's full name, gender, date of birth, UPN and postcode** to be uploaded to Tapestry: Y / N

I give consent to photographs and videos of my child being uploaded to Tapestry Online Learning Journal: Y / N

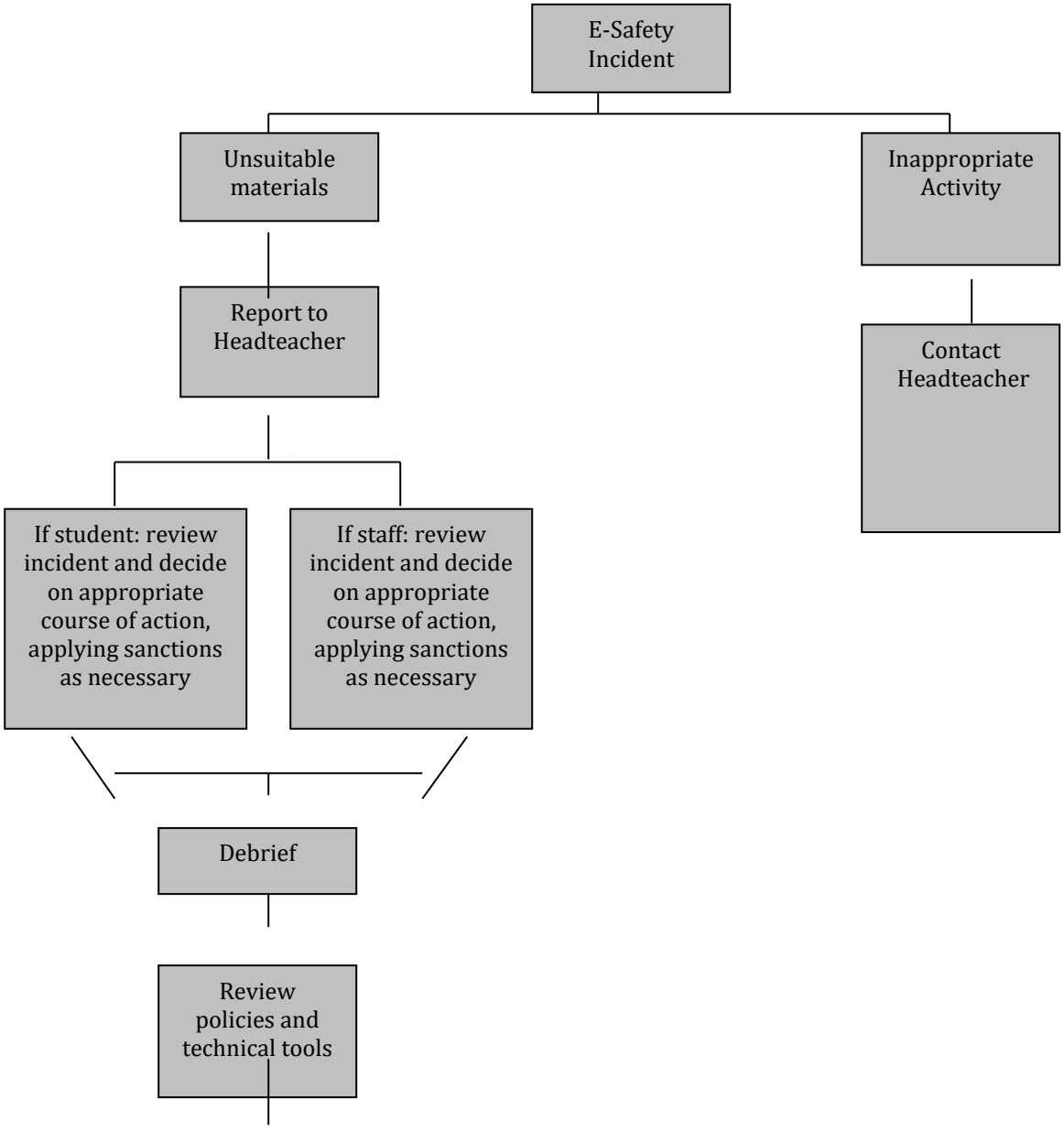
I consent to photographs containing my child's image being included in other children's learning journals: Y / N

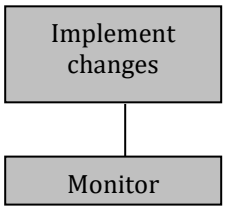
I agree to treat photographs containing images of other children as well as my own for my own personal use only. I understand that the information cannot be shared with others, or published in any way. For example, any such photographs **cannot** be posted on a social networking site or displayed in a public place. Y / N

CHILD'S NAME_____ DATE:_____

PARENT/CARER NAME_____PARENT/CARER SIGNATURE: _____

Appendix B: Flowchart for responding to ESafety incidents





Appendix C: ESafety Audit

This quick self-audit will help the senior management team (SMT) assess whether the eSafety basics are in place.

Has the school an eSafety Policy that complies with CYPD guidance?	Y/N
Date of latest update:	
The Policy was agreed by governors on:	
The Policy is available for staff at:	
And for parents at:	
The designated Child Protection Teacher/Officer is:	
The eSafety Coordinator is:	
Has eSafety training been provided for both pupils and staff?	Y/N
Is the Think U Know training being considered?	Y/N
Do all staff sign an ICT Code of Conduct on appointment?	Y/N
Do parents sign and return an agreement that their child will comply with the School eSafety Rules?	Y/N
Have school eSafety Rules been set for pupils?	Y/N
Are these Rules displayed in all rooms with computers?	Y/N
Is Internet access provided by an approved educational Internet service provider and complies with DCSF requirements for safe and secure access?	Y/N
Has the school filtering policy been approved by SMT?	Y/N

Is personal data collected, stored and used according to the principles of the Data Protection Act?	Y/N
Are staff with responsibility for managing filtering, network access and monitoring adequately supervised by a member of SMT?	Y/N

Appendix D: Are you an ESafe school?

Do all your staff...	Does your school...
☐ Understand e-safety issues and risks? ☐ Receive regular training and updates? ☐ Know how to escalate an issue of concern? ☐ Know how to keep data safe and secure? ☐ Know how to protect themselves online? ☐ Know how to conduct themselves professionally online? ☐ Know about the updated e-safety guidance for QTS standard Q21: Health and well-being?	☐ Have a nominated e-safety co-ordinator? ☐ Audit its e-safety measures? ☐ Have a robust AUP? ☐ Use a Becta accredited supplier for internet services? ☐ Include e-safety measures in Section 4b of your SEF? ☐ Keep an incident log and monitor your measures? ☐ Handle cyberbullying issues well? ☐ Raise awareness of the issues, e.g. through holding an assembly?
Do your learners...	**Do your parents and governors...**
☐ Understand what safe and responsible online behaviour means? ☐ Receive e-safety education at appropriate places across the curriculum? ☐ Get the opportunity to improve their digital literacy skills? ☐ Know the SMART rules? ☐ Know how to report any concerns they may have?	☐ Understand e-safety issues and risks? ☐ Understand their roles and responsibilities? ☐ Receive regular training and updates? ☐ Understand how to protect their children in the home?

Appendix E: Website log

Request to **unblock** a website to be used by Staff and/or Pupils for educational purposes.

Website Address	Reason	Staff	Date	Agreed Y/N	H/T Sig

Request to **block** a website.

Website Address	Reason	Staff	Date		H/T Sig

Appendix F: eSafety Incident Log (see safe-guarding files kept by the child protection officer and the cross – referencing sheets showing any incidents and actions.

Date	Staff	Incident	Action