Easton Royal Academy

Online Safety Handbook

2024 - 2025

Schedule for Monitoring

The implementation of this Online Safety policy will be monitored by the:	*Principal and link governor for safeguarding using:* • *Annual county safeguarding audit (online section) Summer term*
Excalibur Academies Trust will monitor this policy and our practices	• *As part of their Safeguarding review work*
The Local Committee will receive a report on the implementation of the online safety handbook and the effectiveness of online safety at Easton Royal Academy	• *Annually by the Safeguarding link governor (as part of the safeguarding link report)*
The Online Safety Handbook will be reviewed annually in the summer term, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	*Summer 2025*
Should serious online safety incidents take place, the following external persons / agencies should be informed:	*Beck Stubbs (DSL)* *or* *Julie McKay (DDSL)* *Wiltshire MASH*

The school will monitor the effectiveness of online safety practices using:

- Log of reported incidents
- Surveys and face to face discussion with:
    - Children
    - Parents
    - Staff

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the *school / academy*:

Local Committee Members

LCMs are responsible for reviewing the effectiveness of the online safety practice at Easton Royal Academy. A member of the *LC* has taken on the role of Safeguarding (including *Online Safety) Link LCM.* The role of the Safeguarding (and online safety) link LCM includes:

- Meetings with the Principal/DSL (twice a year)
- Attendance at Online Safety presentation evenings for parents
- Reporting to LGB on results of the annual Wiltshire safeguarding audit and the annual EAT audit.

Principal

- The *Principal* has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to teaching and support staff.
- *The Principal is responsible for ensuring that all relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.*
- *The principal will provide statistics to the local governing body about reported incidents related to online safety as part of the context table on the bimonthly principal's report.*
- *The principal will support link governor visits and provide necessary information and evidence.*

In addition, as designated safeguarding lead, the Principal should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- online-bullying

Network Manager / Technical staff

The Network Manager / Technical Staff responsible for ensuring:

- that the *school's* technical infrastructure is secure and is not open to misuse or malicious attack
- that the *school* meets required online safety technical requirements and any Online Safety Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- *the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person*
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the *IT is effectively monitored and* attempted misuse can be reported to the *Principal*.

Teaching and Support Staff

Are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current *school* Online Safety practices
- They have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- They report any suspected misuse or problem to the *Principal*
- All digital communications with children should be on a professional level *and only carried out using official school systems*
- Online safety issues are embedded in all aspects of the curriculum and other activities
- Children understand the school expectations about IT use and now how to stay safe online.
- They monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school.
- *In lessons where internet use is pre-planned, children should be guided to sites checked as suitable for their use and that children are aware of the use of 'Hector's World' in situations when inappropriate context arises.*

Children:

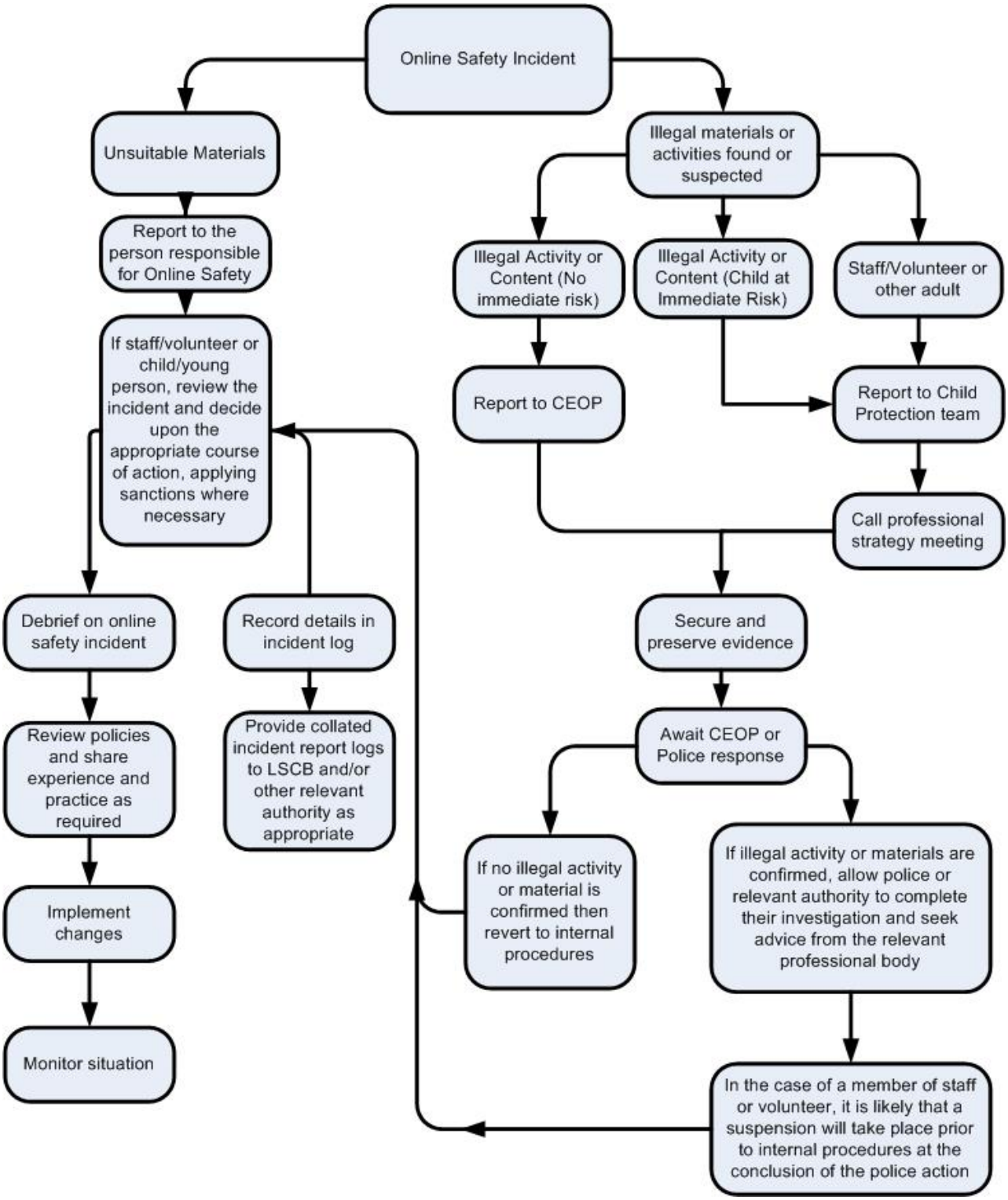
- Are responsible for using the *school* IT systems in accordance with the Acceptable Use Agreement (AUA)
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the *school's* Online Safety reach and responsibility covers their actions out of school, if related to their membership of the school
- Should be able to talk about online safety at their own level (including the childnet 'SMART' rules for KS2)

Parents / Carers

Parents play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The *school* will take every opportunity to help parents understand these issues through *parents' workshops, letters, website and information about national online safety campaigns / literature.*

Illegal Online Incidents - Flowchart

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school guidelines. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority / Academy Group or national / local organisation (as relevant).
    - Police involvement and/or action
- If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - incidents of ‘grooming’ behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism
    - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the *school* and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

Acceptable Use Agreement: Children

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers or iPads.
- I will only do activities or visit sites that a teacher or suitable adult has told or allowed me to visit.
- I will take care of the computer and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.
- If I see something that worries or upsets me on the screen, I will press hector and then tell and adult straight away.
- I know that I also have to behave in a responsible way on the internet at home and school might get involved if I break the rules.
- I know that if I break the rules I might not be allowed to use a computer or iPad.

Signed (child, if in Y2 or above):_____

Signed (parent): _____

Responding to IT misuse