RED OAKS
PRIMARY SCHOOL
Aspire Achieve Grow

16/03/2021

Online Safety Policy

Review Date	Version number	Reviewer/Owner (post holder)	Approved by (Committee)	Signature
March 2021	1	James Lee		

Contents

1. Introduction

The Trust intends and expects that all decisions around the use of Trust resources will be underpinned at all times by its vision and values:

Our aim:

To create centres of educational excellence that inspire all pupils to turn their potential into performance

To achieve this our schools will:

Provide a broad and balanced curriculum that allows pupils to develop their talents and ambitions

Deliver the highest quality learning opportunities facilitated by excellent teachers

Inspire our pupils to become confident, motivated and respectful individuals ready to make a positive contribution to society

The Trust will support our schools by:

Maximising the resources and expertise available to individual schools

Providing a platform for the sharing of excellent practice

Challenging and developing staff to turn their potential into performance

1.1. Aims and Scope

This policy is to be read in conjunction with the school's ICT Systems Security Policy/Use of Camera Technology/Mobile Phones Policy and Data Protection Policies)

'Red Oaks Primary School is strongly committed to protecting and safeguarding children
and expects all staff and volunteers to embrace this commitment'

<u>Our Aims</u>

- To empower children to stay safe in our digital world; by educating them about and building their resilience to the risks to which they are exposed, so that they have the confidence and skills to face and deal with these risks.
- To value and keep up to date with the use of new technologies to enhance learning.
- To deliver online safety throughout the curriculum.
- To support and develop children's learning and understanding of our whole school online safety rules (see Appendix 1).
- To support parents in understanding the issues and risks associated with children's use of digital technologies.
- To ensure that parents are aware of the procedures for online safety within school.

- To support parents in promoting online safety messages in home use of ICT.
- To support staff; including extended schools service providers, in understanding the issues & risks associated with use of ICT; through school policies, procedures & training.
- To ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- To ensure online safety incidents are logged, monitored & reviewed on CPOMS to inform future online safety developments.
- To ensure that the school infrastructure/network is safe and secure.
- To ensure all ICT users adhere to the relevant Acceptable Use Policies.
- To involve pupils in the education of others through our school Cyber Mentors.
- Achieving these aims are the responsibility of everybody who works with our pupils; under the guidance and direction of the Online Safety Co-ordinator, Head Teacher (Rachel Surch), Safeguarding Governor and Director of IT (Geoff Bryan).

Monitoring and Review

Ensuring the online safety of the members of our school community requires a whole school approach. This policy has therefore been written in consultation with the following stakeholders:

- School Online Safety Co-ordinator
- Head Teacher
- Teachers
- Support Staff
- ICT Technician
- Safeguarding Governor
- Governing Body
- Parents/carers
- Community Users, e.g. breakfast club supervisors/children
- Pupils

1.2. Other linked Policies

- ICT Systems Security Policy
- Use of Camera Technology
- Mobile Phones Policy
- Data Protection Policies
- Child Protection Policy
- School Behaviour and Learning Charter
- Anti-bullying Policy
- Pupil Acceptable Use Policy
- Exa Networks Internet Filtering Policy

2. Policy Statement

Our pupils are growing up in an exciting digital age, which we at Red Oaks are keen to embrace. These new technologies are integral to their lives, both inside and outside school; now and in the future, and we believe they are key to preparing our children for lifelong learning, raising educational standards and promoting pupil achievement.

It is their right to have safe online access and part of our duty of care to ensure that they are able to use the internet and related communications technologies appropriately and safely. It is our duty to educate children when they are in our care and educate them for when they are not. It is fundamental to safeguarding children that we educate them to assess and deal with risk appropriately.

2.1. Policy Terms

All users of ICT at Red Oaks will be asked to sign an appropriate ICT Systems Security/Acceptable Use Policy (AUP). If these policies aren't adhered to, the procedures and actions outlined in Appendix 2 must be followed. Please note that the team at Red Oaks take all incidents of inappropriate online safety behaviour very seriously and will inform parents/carers of incidents of inappropriate online safety behaviour that take place both inside and outside of school. Please also refer to Red Oaks' School Behaviour and Learning Charter.

The school will monitor the impact of this policy through:

- Pupil interviews
- Work scrutiny through Computing folders
- Online safety Incident information from CPOMS (School Online Safety Co-ordinator/ICT Technician/Safeguarding Governor/Head Teacher)
- Exa Networks (from July 19) monitoring grids of internet activity (including sites visited)
- Review meetings involving relevant stakeholders as outlined above
- Progress towards evidence for 360° Safe self-assessment tool
- Surveys/questionnaires which will be conducted where/when the school feel appropriate, e.g. parent/teacher surveys
- The work of our school Cyber Mentors
- This policy will be reviewed annually with relevant stakeholders, where relevant. Please note this policy links with the following policies:

.

Appendix 1 – Our school Online Safety Rules

If you share,
it’s always out there,
stop and wait,
Don’t spread the hate,
Ever in doubt,
Shout it out!

Appendix 2 – Flow chart on dealing with Online Safety incidents

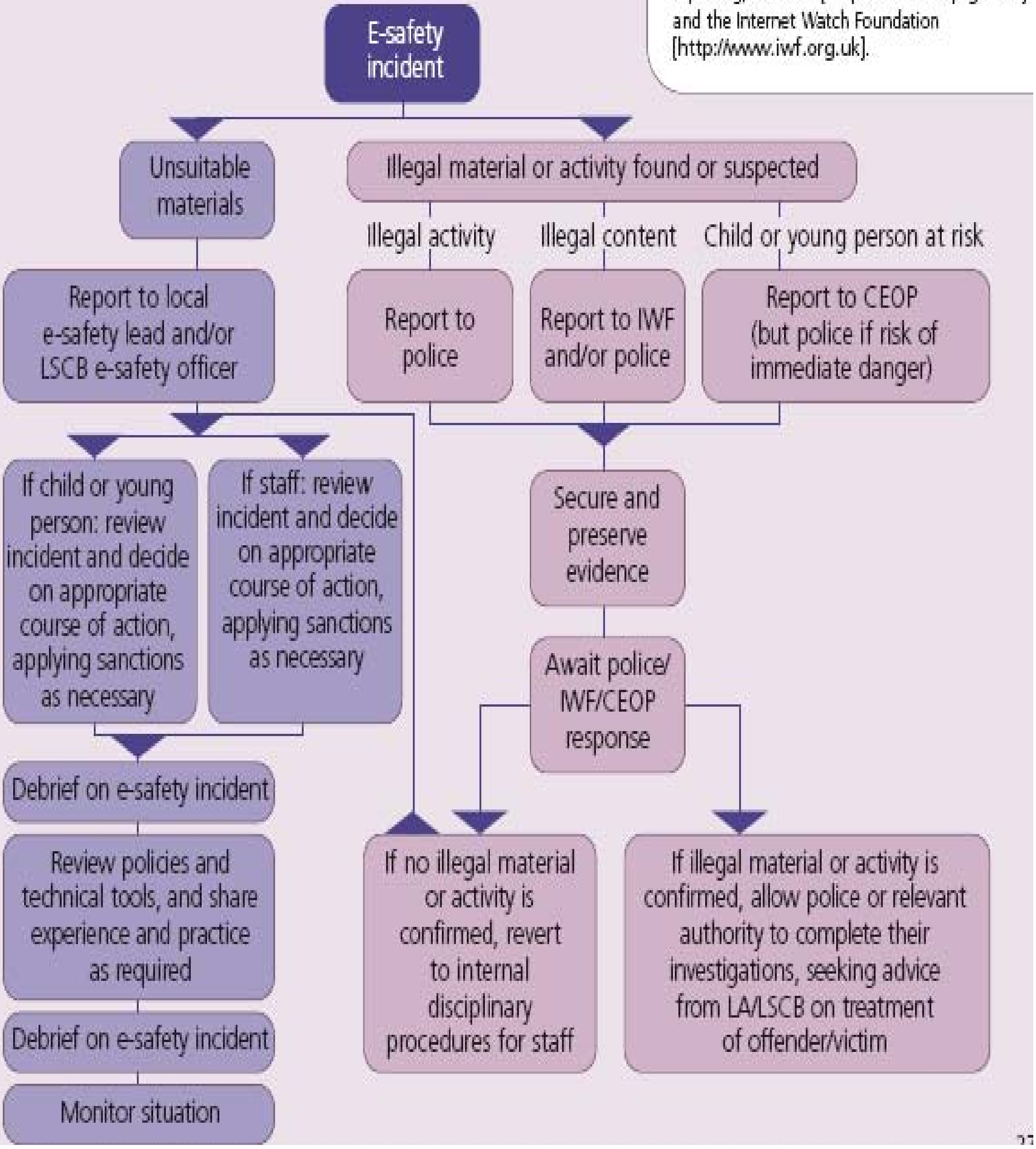
Should there be a serious Online Safety allegation, the Online Safety Co-ordinator and/or Head Teacher must be informed and the procedure outlined in this Appendix and Red Oaks' acceptable behaviour/disciplinary procedures will be followed as appropriate.

ALL Online Safety incidents involving children must be recorded in our Online Safety Incident Reporting Log on CPOMS alerting the Online Safety Coordinator. Where incidents are of a sensitive nature, pupils' anonymity should be maintained.

appendix B

flowchart for responding to e-safety incidents

Note: this flowchart originally appeared as 'Flowchart for responding to internet safety incidents in school' in the Becta publication *E-safety: Developing whole-school policies to support effective practice*. We have revised and updated it to include additional lines of reporting, to CEOP [http://www.ceop.gov.uk] and the Internet Watch Foundation [http://www.iwf.org.uk].



E-safety incident

Unsuitable materials

Report to local e-safety lead and/or LSCB e-safety officer

If child or young person: review incident and decide on appropriate course of action, applying sanctions as necessary

If staff: review incident and decide on appropriate course of action, applying sanctions as necessary

Debrief on e-safety incident

Review policies and technical tools, and share experience and practice as required

Debrief on e-safety incident

Monitor situation

Illegal material or activity found or suspected

Illegal activity

Illegal content

Child or young person at risk

Report to police

Report to IWF and/or police

Report to CEOP (but police if risk of immediate danger)

Secure and preserve evidence

Await police/ IWF/CEOP response

If no illegal material or activity is confirmed, revert to internal disciplinary procedures for staff

If illegal material or activity is confirmed, allow police or relevant authority to complete their investigations, seeking advice from LA/LSCB on treatment of offender/victim

Appendix 2 List of Possible Incidents -Pupils

	Possible consequences:							
Possible Incidents:	Record in Online Safety Incident Log	Refer to Class Teacher/ Head of Key Stage	Refer to Head Teacher	Refer to Police	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction e.g. loss of privileges/ exclusion
Deliberately accessing or trying to access material that could be considered illegal	☒	☒	☒	☒	☒	☒	☒	☒
Using school computers to play non-educational games	☒	☒	□	□	□	□	☒	□
Unauthorised use of camera technology/ mobile phone / digital camera / other handheld device	☒	☒	□	□	□	□	☒	□
Unauthorised use of social networking / instant messaging / personal email	☒	☒	□	□	□	□	☒	□
Unauthorised downloading/uploading of files	☒	☒	□	□	□	□	☒	□
Allowing others to access school network by sharing username and passwords	☒	☒	□	□	□	□	☒	□
Attempting to access/accessing the school network, using another pupil's account	☒	☒	□	□	□	□	☒	□
Attempting to access or accessing the school network, using the account of a member of staff	☒	☒	☒	□	☒	□	☒	□
Attempting to access or accessing another person's email account	☒	☒	☒	□	☒	☒	☒	☒
Corrupting/destroying other users' data	☒	☒	□	□	□	□	☒	□
Sending an email, text/instant message of an offensive, harassing or bullying nature	☒	☒	☒	□	☒	□	□	☒
Spreading untrue/offensive rumours related to online behaviour	☒	☒	☒	□	☒	□	☒	☒
Actions which could bring the school into disrepute/ breach the integrity of its ethos	☒	☒	☒	□	□	☒	☒	☒
Using proxy sites or other means to subvert the school's filtering system	☒	☒	☒	□	☒	☒	□	☒

Accidentally accessing offensive/ pornographic material & failing to report the incident	☒	☒	□	□	☒	□	□	□
Deliberately accessing or trying to access offensive or pornographic material	☒	☒	☒	☒	☒	☒	☒	☒
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	☒	☒	□	□	□	□	☒	□
Continued infringements of the above, following previous warnings or sanctions	☒	☒	☒	□	☒	☒	□	☒

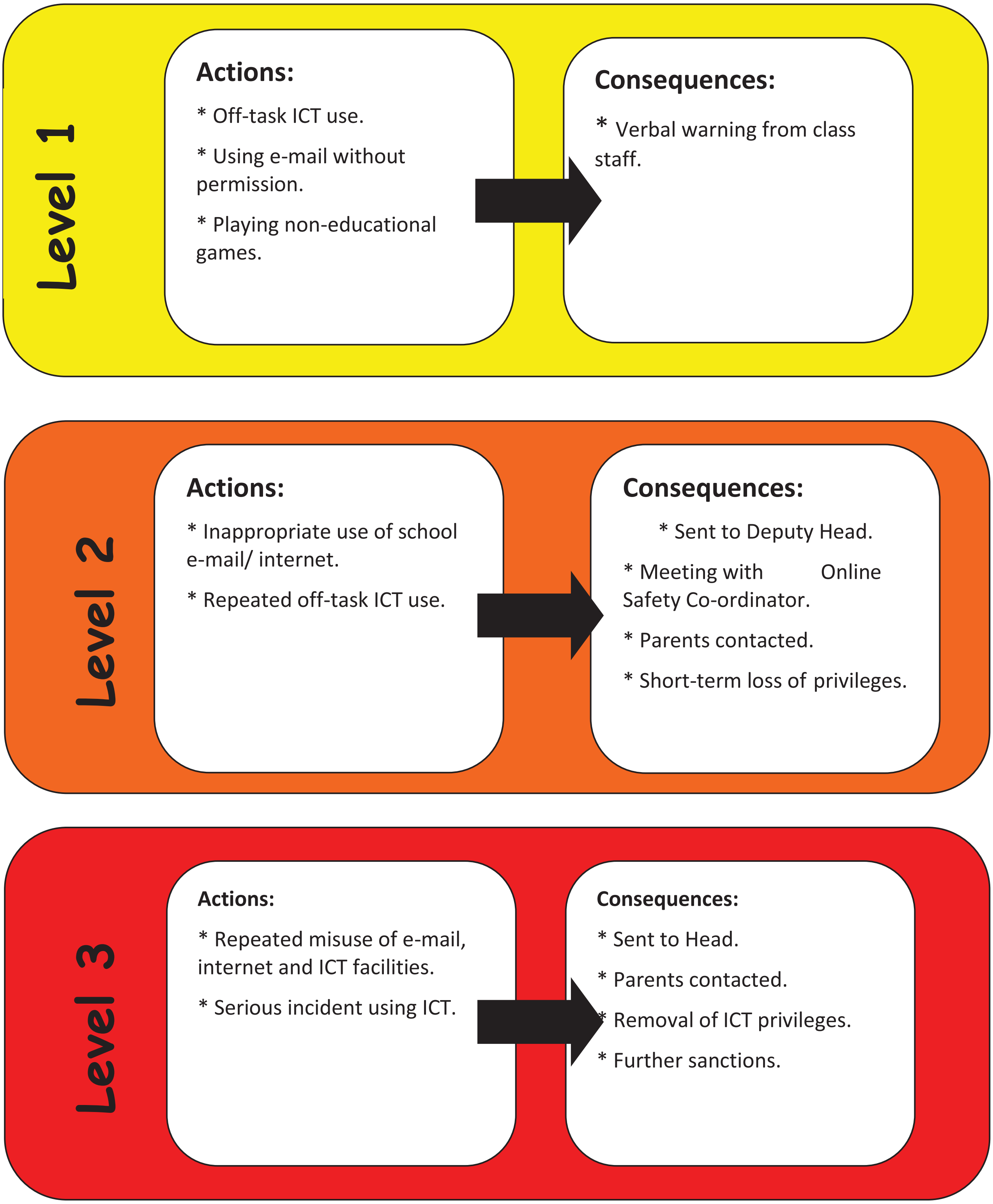
Please also refer to the summary of this policy which is displayed in all KS2 classrooms.

Appendix 2 List of Possible Incidents -Staff

Possible Incidents:
Deliberately accessing or trying to access material that could be considered illegal
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email
Making any reference to Red Oaks Primary School on any social media platform – this includes referencing the school by name to either celebrate successes or make negative comments.
Advertising school events on personal or public social media pages.
Unauthorised downloading/uploading of files
Allowing others to access school network by sharing username & passwords/ attempting to access or accessing the school network, using another person's account
Careless use of personal data e.g. holding or transferring data in an insecure manner
Deliberate actions to breach data protection or network security rules
Corrupting/destroying other users' data/ causing deliberate damage to hardware/ software
Sending an e-mail, text or instant message that is regarded as offensive, harassment or of a bullying nature
Using personal e-mail / social networking / instant messaging / text messaging to carry out digital communications with pupils
Actions which could compromise the staff member's professional standing
Actions which could bring the school into disrepute/breach the integrity of its ethos
Using proxy sites or other means to subvert the school's filtering system
Accidentally accessing offensive/ pornographic material & failing to report the incident
Deliberately accessing or trying to access offensive or pornographic material
Breaching copyright or licensing regulations
Continued infringements of the above, following previous warnings or sanctions
Using personal camera technology/their mobile phone to take photographs of children

All of the above actions by staff are not acceptable. All staff have signed to adhere to the Red Oaks ICT Systems Security Policy which clearly outlines the school's standards and expectations in relation to Online Safety. Should a member of staff breach the above policy or the school's Online Safety or Camera Technology/Mobile Phone Policy, incidents should be referred to the Head Teacher in the first instance who would then escalate as appropriate (e.g. reporting to the ICT Technician for action or to the Local Authority/Police) and take the necessary disciplinary action, if appropriate.

Appendix 4 Consequences of not following Red Oaks' Online Safety Policy



Level 1

Actions:

* Off-task ICT use.

* Using e-mail without permission.

* Playing non-educational games.

Consequences:

* Verbal warning from class staff.

Level 2

Actions:

* Inappropriate use of school e-mail/ internet.

* Repeated off-task ICT use.

Consequences:

* Sent to Deputy Head.

* Meeting with Online Safety Co-ordinator.

* Parents contacted.

* Short-term loss of privileges.

Level 3

Actions:

* Repeated misuse of e-mail, internet and ICT facilities.

* Serious incident using ICT.

Consequences:

* Sent to Head.

* Parents contacted.

* Removal of ICT privileges.

* Further sanctions.

A pupil can go straight to Level 2 or Level 3 without passing through the preceding levels if the offence is considered serious enough to warrant a sanction at a higher level.