Oak Lodge Primary School

Online Safety Policy

Document Detail	
Category:	Online Safety
Authorised By:	Head Teacher
Status:	Approved
Approved By:	LGB
September 2024	September 2024
Next Review Date:	September 2025
Version:	1

Contents

1. Introduction

Oak Lodge Primary School recognises that internet, mobile and digital technologies provide positive opportunities for children and young people to learn, socialise and play whilst understanding the challenges and risks. The digital world is an amazing place, but with few rules. It is vast and fast moving and young people's future economic success may be partly dependent on their online skills and reputation. We are, therefore, committed to ensuring that **all** pupils, staff and governors will be supported to use internet, mobile and digital technologies safely. This is part of our safeguarding responsibility. Staff are aware that some pupils may require additional support or teaching, including reminders, prompts and further explanation to reinforce their knowledge and understanding of online safety issues.

We are also committed to ensuring that all those who work with children and young people, including their parents/carers, are informed about the ever-changing risks so that they can take an active part in helping children and young people navigate the online world safely and confidently.

2. Responsibilities

The headteacher and governors have ultimate responsibility to ensure that appropriate online safety policy and practice is embedded and monitored.
All breaches of this policy must be reported to a member of SLT.
All breaches of this policy that may have put a child at risk must also be reported to a Designated Safeguarding Lead.

Organisations that are renting space from the school and are a totally separate organisation should have and follow their own online safety policy and acceptable use agreements. However, if the organisation has any access to the school network, cloud-based services and/or equipment then they must adhere to the school's online safety procedures and acceptable use agreements.

If the organisation is operating in school time or when pupils are on site in the care of the school, then the safeguarding of pupils is paramount and the organisation must adhere to the school's online safety procedures and acceptable use agreements.

3. Scope of policy

The policy applies to:

- pupils
- parents/carers
- teaching and support staff
- school governors
- peripatetic teachers/coaches, supply teachers, student teachers
- visitors
- volunteers
- voluntary, statutory or community organisations using the school's facilities

The school provides online safety information for parents/carers, for example, through the website, in newsletters and at events. It is important that parents/carers understand their key role in supporting their child/ren to behave appropriately and keep themselves safe online.

This policy, supported by its acceptable use agreements, is intended to protect the interests and safety of the whole school community. It is linked to the following other school policies and documents:

- Safeguarding
- Keeping Children Safe in Education
- GDPR
- Health and safety
- Home–school agreement
- Behaviour and Relationships policy
- Anti-bullying

4. Policy and procedure

The school seeks to ensure that internet, mobile and digital technologies are used effectively and safely, for their intended educational purpose, in ways that will not infringe legal requirements or create unnecessary risk.

The school expects everyone to use internet, mobile and digital technologies responsibly according to the conditions set out in this policy. This policy also includes expectations on appropriate online behaviour and use of technology outside of school for pupils, parents/carers, staff and governors and all other visitors to the school.

Visiting online sites and downloading

- Staff must preview sites, software and apps before their use in school or before using or recommending them to pupils.

Users must not:

- Engage in any age-inappropriate digital activity of any type
- Promote hatred, discrimination of any kind or illegal activity
- Use school hardware/software/Wifi facilities inappropriately or for private business.

Storage of Images

Photographs and videos provide valuable evidence of pupils' achievement and progress in a variety of contexts and can be used to celebrate the work of the school (e.g. see saw). In line with GDPR they are used only with the written consent of parents/carers which is secured in the first instance on a child's entry to the school. Records are kept on file and consent can be changed by parents/carers at any time.

Photographs and images of pupils are only stored on the school's agreed secure networks which include some cloud-based services.

Parents/carers should note that there may be some children who are at risk and must not have their image put online and others who do not want their image online. For these reasons parents/carers must follow the school's Acceptable Use Agreement and refrain from taking or posting online photographs of any member of the school community, other than their own child/ren.

Staff and other professionals working with pupils, must only use school equipment to record images of pupils whether on or off site. Permission to use images of all staff who work at the school is sought on induction and a written record is located in the personnel file.

Use of personal mobile devices (including phones)

The school allows staff, including temporary and peripatetic staff, and visitors to use personal mobile phones and devices but never in the presence of pupils. Under no circumstance does the school allow a member of staff to contact a pupil using their personal device. If a parent/carer is contacted, the caller's number must be withheld.

Parents/carers may not use personal mobile phones and devices in school unless otherwise informed, e.g. for specific events and activities.

- Pupils are allowed to bring personal mobile devices/phones to school but these are to be kept securely in the office during the school day. Under no circumstance should pupils use their personal mobile devices/phones to take images of
- any other pupil unless they and their parents have given agreement in advance
- any member of staff
- The school is not responsible for the loss, damage or theft of any personal mobile device that is brought into school.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

Reporting incidents, abuse and inappropriate material

There may be occasions in school when either a pupil or an adult receives an offensive, abusive or inappropriate message or accidentally accesses upsetting or abusive material. When such a situation occurs the pupil or adult must report the incident immediately to the first available member of staff. Where such an incident may lead to significant harm, safeguarding procedures should be followed. The school takes the reporting of such incidents seriously and where judged necessary, one of the Designated Safeguarding Leads will refer details to social care or the police.

5. Curriculum

Online safety is fully embedded within our curriculum. The school provides a comprehensive age-appropriate curriculum for online safety which enables pupils to become informed, safe and responsible.

The curriculum is flexible and can respond to any immediate online safety issues and risks as they emerge.

It is necessary for pupils to develop skills of critical awareness, digital resilience and good online citizenship to enable them to use internet, mobile and digital technologies safely and responsibly.

6. Staff and Governor Training

Staff and governors are trained to fulfil their roles in online safety. The school provides regular training to improve their knowledge and expertise in the safe and appropriate use of internet, mobile and digital technologies.

New staff are provided with a copy of the online safety policy and must sign the school's Acceptable Use Agreement as part of their induction.

Any organisation working with children and based on the school premises are also provided with a copy of the online safety policy and required to sign the Acceptable Use Agreement

Peripatetic staff, student teachers and regular visitors are provided with a copy of the online safety policy and are required to sign the Acceptable Use Agreement (Appendix B).

Guidance is provided for occasional visitors, volunteers and parent/carer helpers (Appendix E).

7. Working in Partnership with Parents/Carers

The school works closely with families to help ensure that children can use internet, mobile and digital technologies safely and responsibly both at home and school. The support of parents/carers is essential to implement the online safety policy effectively and help keep children safe.

Parents/carers are asked to read, discuss and co-sign with each child the Acceptable Use Agreement. A summary of key parent/carer responsibilities will also be provided and is available in Appendix F. The Acceptable Use Agreement explains the school's expectations and pupil and parent/carer responsibilities.

8. Records, monitoring and review

The school recognises the need to record online safety incidents and to monitor and review policies and procedures regularly in order to ensure they are effective and that the risks to pupils and staff are minimised.

All breaches of this policy must be reported and all reported incidents will be logged. All staff have the individual responsibility to ensure that incidents have been correctly recorded, acted upon and reported.

The school supports pupils and staff who have been affected by a policy breach. Where there is inappropriate or illegal use of internet, mobile and digital technologies, this will be dealt with under the school's behaviour and disciplinary policies as appropriate. Breaches may also lead to criminal or civil proceedings.

Governors receive termly summary data on recorded online safety incidents for monitoring purposes. In addition governors ensure they have sufficient, quality information to enable them to make a judgement about the fitness for purpose of this policy on an annual basis.

Appendix A - Online Safety Acceptable Use Agreement - Staff, Governors and student teachers (on placement or on staff)

You must read this agreement in conjunction with the online safety policy and the GDPR policy. Once you have read these, you must sign and submit this agreement and it will be kept on record in the school. You should retain your own copy for reference. This forms part of your professional and safeguarding responsibilities.

Internet, mobile and digital technologies are part of our daily working life and this agreement is designed to ensure that all staff and governors are aware of their responsibilities in relation to their use. All staff, student teachers and governors are expected to adhere to this agreement and to the online safety policy. Any concerns or clarification should be discussed with Mrs Lowton. Breaches will be investigated, recorded and, where appropriate, disciplinary procedures will apply and police involvement will be sought.

Internet Access

I will not access or attempt to access any sites that contain any of the following: child abuse; pornography; discrimination of any kind; promotion of prejudice against any group; promotion of illegal acts; any other information which may be illegal or offensive. Inadvertent access on school equipment must be treated as an online safety incident, reported to Mrs Lowton and an incident report completed.

Online conduct

I will ensure that my online activity, both in and outside school, will not bring the school, my professional reputation, or that of others, into disrepute.

I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory. Exceptionally, use of controversial material as part of the curriculum should be planned and approved on every occasion (see policy).

I will report any accidental access to or receipt of inappropriate materials or filtering breach to Mrs Lowton.

I understand that all my use of the internet and other related technologies can be traced and monitored and, should it be required, must be made available to my line manager, headteacher and others as required.

I will not give out my personal contact and online account information such as phone numbers, email address, and social media account details to pupils and/or parents/carers.

Social networking

I understand the need to separate my professional role from my private friendships; in my professional capacity I will not become 'friends' with parents/carers or pupils on social networks. Where my school role is my only connection to an individual, private online contact is unacceptable with parents/carers or pupils.

When using social networking for personal use I will ensure my settings are not public. My private account postings will never undermine or disparage the school, its staff, governors, parents/carers or pupils. Privileged information must remain confidential.

I will not open e-mails when the Interactive Whiteboard is on or children are nearby.

I will not upload any material about or references to the school or its community on my personal social networks.

Passwords

I understand that there is no occasion when a password should be shared with a pupil or anyone who is not a staff member.

Data protection

I will follow requirements for data protection as outlined in our GDPR policy.

Images and videos

I will only upload images or videos of staff, pupils or parents/carers onto school approved sites where specific permission has been granted.

I will not take images, sound recordings or videos of school events or activities on any personal device.

Use of email

I will use my school email address or governor hub for all school business. All such correspondence must be kept professional and is open to Subject Access Requests under the Freedom of Information Act. I will not use my school email addresses or governor hub for personal matters or non-school business.

Use of personal devices

I understand that as a member of staff I should at no time put myself in a position where a safeguarding allegation can be made against me as a result of my use of personal devices.

I will only use approved personal devices away from pupils.

Additional hardware/software

I will not install any hardware or software on school equipment without permission of the school technical support.

Promoting online safety

I understand that online safety is the responsibility of all staff and governors and I will promote positive online safety messages at all times including when setting homework or providing pastoral support.

I understand that it is my duty to support a whole school safeguarding approach and will report any inappropriate or concerning behaviour (of other staff, governors, visitors, pupils or parents/carers) to the head teacher.

Classroom management of internet access

I will pre-check for appropriateness all internet sites used in the classroom this will include the acceptability of other material visible, however briefly, on the site. I will not free-surf the internet in front of pupils. I will also check the appropriacy of any suggested sites suggested for home learning.

If I am using the internet to teach about controversial issues I will use professional judgement.

Video conferencing

I will only use the conferencing tools that have been identified and risk assessed by the school.

User signature

I agree to follow this Acceptable Use Agreement and to support online safety throughout the school. I understand this forms part of the terms and conditions set out in my contract of employment (staff members only) and/or my responsibilities as a governor.

Signature …….…… Date ……

Full Name …….... (printed)

Job title ……

Appendix B - Online Safety Acceptable Use Agreement - Supply teachers

Oak Lodge Primary School

Designated Safeguarding Lead (DSL/DDSL):

Mrs Diane Lowton
Mrs Tracy Jackson
Mrs Linda Allen
Mr Daniel Grice

This agreement forms part of your professional and safeguarding responsibility in the school. You must read and sign this agreement. This will be kept on record and you should retain your own copy for reference.

Internet, mobile and digital technologies are part of our daily working life and this agreement is designed to ensure that all staff and governors are aware of their responsibilities in relation to their use. You are expected to adhere to this agreement. Any concerns or clarification should be discussed with a DSL. Breaches will be investigated, recorded and, where appropriate, disciplinary procedures will apply and police involvement will be sought.

The school's online safety policy will provide further detailed information as required.

Internet Access
``
I will not access or attempt to access any sites that contain any of the following: child abuse; pornography; discrimination of any kind; promotion of prejudice against any group; promotion of illegal acts; any other information which may be illegal or offensive. Inadvertent access on school equipment must be treated as an online safety incident, reported to the online safety lead and/or DSL and an incident report completed.

Online conduct

I will ensure that my online activity, both in and outside school, will not bring the school, my professional reputation, or that of others, into disrepute.

I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory. Exceptionally, use of controversial material as part of the curriculum should be planned and approved on every occasion (see policy).

I will report any accidental access to or receipt of inappropriate materials or filtering breach to a DSL.

I understand that all my use of the internet and other related technologies can be traced and monitored and, should it be required, must be made available to my line manager, headteacher and others as required.

I will not give out my personal contact and online account information such as phone numbers, email address, and social media account details to pupils and/or parents/carers.

Social networking

I understand the need to separate my professional role from my private friendships; in my professional capacity I will not become 'friends' with parents/carers or pupils on social networks. Where my school role is my only connection to an individual, private online contact is unacceptable with parents/carers or pupils.

In my professional role in the school, I will never engage in 1-1 exchanges with pupils or parent/carers on personal social network sites.

My private account postings will never undermine or disparage the school, its staff, governors, parents/carers or pupils. Privileged information known as a result of my work in the school must remain confidential.

I will not upload any material about or references to the school or its community on my personal social networks.

Passwords

I must clarify what access I may have to the internet and/or school systems. If I have access of any kind, I understand that there is no occasion when a password should be shared with a pupil or anyone who is not a staff member.

Data protection

I will follow all requirements for data protection explained to me by the school. These include:

- I must consult with the school before making any recordings, photographs and videos. Once agreed, these must be made on a school device.

- I understand that there are strict controls and requirements regarding the collection and use of personal data. I will follow all requirements regarding GDPR.

Images and videos

I will not take images, sound recordings or videos of tuition or wider school activities on any personal device. School devices can be used for this purpose.

Use of Email

I will only use my professional email address for all school business. All such correspondence should be kept professional and is open to Subject Access Requests under the Freedom of Information Act. I will not use my professional email addresses for personal matters.

Use of personal devices

I understand that when working in the school I should at no time put myself in a position where a safeguarding allegation can be made against me as a result of my use of personal devices.

I will not use personal devices in front of pupils. This therefore precludes use of specialist apps on personal devices. A school device could be used to access specialist apps that support pupil learning.

Additional hardware/software

I will not install any hardware or software on school equipment.

Promoting online safety

I understand that online safety is part of my responsibility and I will promote positive online safety messages at all times, including when setting homework, rehearsal or skill practice or when providing pastoral support.

I understand that it is my duty to support a whole school safeguarding approach and will report any behaviour (of staff, governors, visitors, pupils or parents/carers) which I believe may be inappropriate or concerning in any way to the DSL.

Classroom management of internet access

I will pre-check for appropriateness, all internet sites used in the classroom; this will include the acceptability of other material visible, however briefly, on the site. I will not free-surf the internet in front of pupils or open e-mails.

User Signature

I agree to follow this Acceptable Use Agreement and to support online safety in my work in the school. I understand this forms part of my company/educational setting/organisation's contract with the school.

Signature …….…….…… Date …….……

Full Name …….... (Please use block capitals)

Job Title/Role …….……

Appendix C - Requirements for visitors, volunteers and parent/carer helpers

(Working directly with children or otherwise)

School name……..…..

DSL ……..…..

This document is designed to ensure that you are aware of your responsibilities when using any form of IT in the school and other aspects of safeguarding in connection with online safety.

Please raise **any** safeguarding concerns arising from your visit immediately with the headteacher and/or DSL

- I understand I may not use my personal mobile phone(s) and other devices with camera functions in school designated areas. My phone will be switched off and out of sight.
- I will not take images, sound recording or videos of school events or activities, on or off site, on any device. Any possible exception must be pre-arranged.
- I will not give out my personal details such as mobile phone number, email address, and social media account details to pupils. Where appropriate I may share my professional contact details with parents/carers provided the DSL or headteacher is informed before I leave the school.
- I understand my visit to the school may give me access to privileged information about pupils, staff, school systems and plans. Such information should never be shared on line, including on social media sites.
- I understand I should not use school equipment to access the internet without prior approval from my contact in the school or the headteacher.
- If working in the classroom, I will pre-check for appropriateness all internet sites I intend to use including checking the acceptability of other material visible on the site. I will not free-surf the internet in front of pupils. If I am in any doubt about the appropriateness of the content I plan to use I will check with my contact in the school.

Appendix D - Online Safety Agreement Primary Pupils

My online safety agreement

- I will ask permission before using digital technologies.
- I will keep my password private.
- I will log out when not using digital technologies.
- I will only take photographs when asked to by my teacher for classwork.
- I will create content for positive reasons.
- I will support my classmates and report negative comments.
- I will check the timer whilst using online platforms.
- I know that poor choices will result in my screen time being reduced.
- I know that all games, platforms and software have age restrictions to keep me safe.
- I agree to all the above terms.

Dear Parent/Carer,

The internet, email, mobile technologies and online resources have become an important part of learning and life. We want all children to be safe and responsible when using any IT. It is essential that children are aware of online risk, know how to stay safe and know where to go to report problems or to get help.

Please read through these online safety rules with your child/ren and talk with them to ensure they understand their importance and what it means for them (and for you). When you have done this, you both need to sign this agreement to say that you agree to follow the rules. Any concerns or explanation can be discussed with DSL team.

Please return the signed sections of this form which will be kept on record at the school.

Pupil agreement

Pupil name……

This agreement is to keep me safe. I have discussed this agreement with my parents/carers and understand the commitment I have made and my responsibilities.

Pupil signature……..

Parent(s)/Carer(s) agreement

Parent(s)/Carer(s) name(s)……

I/we have discussed this agreement, which highlights the associated risks when accessing the internet, mobile and digital technologies, with our child/ren. I/we agree to support them in following the terms of this agreement.

I/we also agree not to share school related information or images online or post material that may bring the school or any individual within it into disrepute.
(Rather than posting negative material online, any parent, distressed or concerned about an aspect of school should make immediate contact with a member of staff. Negative postings about the school would impact on the reputation of the whole school community. Parents are encouraged to report breaches so that we can protect the reputation of the school, staff, pupils and parents).

I/we also agree not to use personal mobile phones and devices in school unless otherwise informed, e.g. for specific events and activities. I/we understand that under no circumstance should images be taken at any time on school premises of anyone other than our own child/ren, unless there is a pre-specified agreement. I/we understand that when on school premises, phones must be out of sight.

Parent(s)/Carer(s) agreement

Parent(s)/Carer(s) name(s)…….

Parent/carer signature……..

Date ……..……

Appendix F - Online safety policy guide - Summary of key parent/carer responsibilities

The school provides online safety information for parents/carers, through the website, in newsletters and at events. It is important that parents/carers understand their key role in supporting children to behave appropriately and keep themselves safe online.

The online safety policy, supported by its acceptable use agreements, is intended to protect the interests and safety of the whole school community.

- Parents/carers are required to support their child in understanding and signing the Online Safety Acceptable Use Agreement for pupils.

- Parents/carers may not use personal mobile phones and devices in school unless otherwise informed, e.g. for specific events and activities. Under no circumstance should images be taken at any time on school premises that include anyone other than their own child, unless there is a pre-specified agreement with individuals and parents/carers. When a parent/carer is on school premises but not in a designated area, their phone/s must be switched off and out of sight.

- All cyberbullying incidents affecting children in the school should be reported immediately. (If the incident involves an indecent image of a child the report must also be made immediately to the police for your own protection.) The school will investigate and respond to all reported cyberbullying incidents, liaising with others where appropriate. No reply should ever be sent to the sender/poster of cyberbullying content. If applicable block the sender and report abuse to the site. Evidence should be retained and shown in school and/or to the police. Evidence should not be forwarded.

- The school may choose to set up social media sites, blogs or have some other online presence in its own name. Parents/carers, however, do not have the right to set up any site, page, chat group or any other online presence that uses the school name or logo in any form.

- Any parent/carer, distressed or concerned about an aspect of school should make immediate contact with a member of staff rather than posting their concerns online. Parents/carers should not share school related information or images online or post material that may bring the school or any individual within it into disrepute. Negative postings about the school would impact on the reputation of the whole school community. Parents/carers are encouraged to report breaches so that we can protect the reputation of the school, staff, pupils and parents/carers.

Please see the full online safety policy in the policies section on the school website.

Appendix G - **Guidance on the process for responding to cyberbullying incidents**

All cyberbullying incidents should be reported and responded to. Where the perpetrator is a member of the school community the majority of cases can be dealt with through mediation and/or disciplinary processes.

The following procedures are recommended:

- Never reply to the sender/poster of cyberbullying content. If applicable, block the sender.
- Incidents should be reported immediately. Pupils should report to a member of staff (e.g. class teacher, headteacher) and staff members should seek support from their line manager or a senior member of staff.
- The person reporting the cyberbullying should save the evidence and record the time and date. This evidence must not be forwarded but must be available to show at a meeting. Under no circumstances should indecent images of children and young people be printed or forwarded as this is a further criminal act. Staff should not ask to see the evidence of reported indecent images of children or young people but must refer this immediately to the police. Any member of staff being shown such evidence should immediately inform their line manager or the headteacher so that the circumstances can be recorded.
- A senior member of staff will meet with the person who has reported the incident and the target, if different, to listen, reassure and support. All relevant facts will be reviewed and documented.
- A senior member of staff will conduct an investigation.
- Anyone found to have cyberbullied will have attention drawn to the seriousness of their behaviour and if necessary, the police will be involved. If the comments are threatening, abusive, sexist, of a sexual nature, constitute a hate crime or are libellous they may well break the law. Online harassment and stalking is also a crime.
- Once evidence has been secured then the person who has cyberbullied will be requested to remove the offending comments/material. Any refusal will lead to an escalation of sanctions.

Appendix H - **Guidance for staff on preventing and responding to negative comments on social media**

The school should make it clear which, if any, social media platforms are used to communicate with parents/carers. If used correctly, parents can use a school's social media site as a source of reliable information. The online safety policy, see especially Appendix F (Online safety policy guide - Summary of key parent/carer responsibilities), clarifies that no other social media platforms should be set up using the school's name or logo.

The school should regularly reinforce with all parties that discussion of school issues on social media platforms, either positive or negative, should not take place as this could bring the school into disrepute and affect families and children. Parents should be encouraged to be good online role models and not post statements written in anger or frustration. Identified routes to raise concerns directly with the school should be used.

If negative comments are posted:

- Collect the facts

  As soon as you become aware of adverse comments relating to the school you need to establish what is being said. It is essential that if you have access to the postings they are secured and retained together with any other evidence. Do not become engaged in responding directly.

  If the allegations against a member of staff or a pupil are of a serious nature, these will need to be formally investigated. This may involve the police and the headteacher will need to follow the school's safeguarding procedures.

  If there is a risk of serious damage to the school reputation or the reputation of individual members of staff, professional legal advice should be sought.

  Adverse comments of any kind are highly demotivating and cause stress and anxiety. It is important that the senior staff reassure and support all staff and/or other affected members of the school community.

- Addressing negative comments and complaints

  Contact the complainants and invite them to a meeting. In the meeting, make sure you have any evidence available.

  The meeting must:

  - Draw attention to the seriousness and impact of the actions/postings;
  - Ask for the offending remarks to be removed;
  - Explore the complainant's grievance;
  - Agree next steps;
  - Clarify the correct complaints procedures.

  If the meeting does not resolve the issue, the parents must be informed that the school will need to take the matter further. This may include:

  - Reporting the matter to the social network site if it breaches their rules or breaks the law;
  - Reporting the matter to the police if it breaks the law, e.g. if the comments are threatening, abusive, malicious, sexist, of a sexual nature, constitute a hate crime or are libellous they may well break the law. Online harassment and stalking is also a crime.

  If inappropriate postings continue or the original material is not removed, a second meeting is advisable to reiterate the seriousness of the matter.

Appendix I - Online safety incident reporting form

Any member of the school community can raise a concern about an online safety incident. If you have witnessed or experienced an incident please complete the form below to help us to address the issue. It is important that you provide as much detail as possible. Once completed please hand this report to the DSL.

Name of person reporting incident:				
Signature:				
Date you are completing this form:				
Where did the incident take place:	Inside school?		Outside school?	
Date of incident(s):				
Time of incident(s):				

Who was involved in the incident(s)?	Full names and/or contact details
Children/young people	
Staff member(s)	
Parent(s)/carer(s)	
Other, please specify	

Type of incident(s) (indicate as many as apply)			
Accessing age inappropriate websites, apps and social media		Accessing someone else's account without permission	
Forwarding/spreading chain messages or threatening material		Posting images without permission of all involved	
Online bullying or harassment (cyber bullying)		Posting material that will bring an individual or the school into disrepute	
Racist, sexist, homophobic, religious or other hate material		Online gambling	
Sexting/Child abuse images		Deliberately bypassing security	
Grooming		Hacking or spreading viruses	
Accessing, sharing or creating pornographic images and media		Accessing and/or sharing terrorist material	
Accessing, sharing or creating violent images and media		Drug/bomb making material	
Creating an account in someone else's name to bring them into disrepute		Breaching copyright regulations	
Other breach of acceptable use agreement, please specify			

Full description of the incident	What, when, where, how?
Name all social media involved	Specify: Twitter, Facebook, Whatsapp, Snapchat, Instagram etc
Evidence of the incident	Specify any evidence available but do not attach.

Thank you for completing and submitting this form.

Appendix J - Online safety incident record

Name of person reporting incident:				
Date of report:				
Where did the incident take place:	Inside school?		Outside school?	
Date of incident(s):				
Time of incident(s):				

Who was involved in the incident(s)?	Full names and/or contact details
Children/young person	
Staff member(s)	
Parent(s)/carer(s)	
Other, please specify	

Type of incident(s) (indicate as many as apply)			
Accessing age inappropriate websites, apps and social media		Accessing someone else's account without permission	
Forwarding/spreading chain messages or threatening material		Posting images without permission of all involved	
Online bullying or harassment (cyberbullying)		Posting material that will bring an individual or the school into disrepute	
Racist, sexist, homophobic, religious or other hate material		Online gambling	
Sexting/Child abuse images		Deliberately bypassing security	
Grooming		Hacking or spreading viruses	
Accessing, sharing or creating pornographic images and media		Accessing and/or sharing terrorist material	
Accessing, sharing or creating violent images and media		Drug/bomb making material	
Creating an account in someone else's name to bring them into disrepute		Breaching copyright regulations	
Other breach of Acceptable Use Agreement			
Other, please specify			

Full description of the incident	What, when, where, how?
Name all social media involved	Specify: Twitter, Facebook, Whatsapp, Snapchat, Instagram etc
Evidence of the incident	Specify any evidence provided but do not attach

Immediate action taken following the reported incident:	
Incident reported to online safety Lead /DSP/ /Headteacher	
Safeguarding advice sought, please specify	
Referral made to HCC Safeguarding	
Incident reported to police and/or CEOP	
Online safety policy to be reviewed/amended	
Parent(s)/carer(s) informed please specify	
Incident reported to social networking site	
Other actions e.g. warnings, sanctions, debrief and support	
Response in the wider community e.g. letters, newsletter item, assembly, curriculum delivery	

Brief summary of incident, investigation and outcome (for monitoring purposes)	

Appendix K - Online safety incident log

Summary details of ALL online safety incidents will be recorded on this form by the online safety lead or other designated member of staff. This incident log will be monitored at least termly and information reported to SLT and governors.

Date & time	Name of pupil or staff member Indicate target (T) or offender (O)	Nature of incident(s)	Details of incident (including evidence)	Outcome including action taken