



Batford Nursery School & Day Care

BATFORD NURSERY SCHOOL Online Safety Policy

Version	3.0
Based on Model Policy	HfL Model Online Safety Policy, June 2020
Review body:	Headteacher
Date issued:	July 2020, reviewed June 2022 – no update; rev July 2024 – see below.
Review frequency:	Two years
Target audience:	All stakeholders

Version	Date	Notes
V 1.0	November 2018	Model policy adopted
V 2.0	October 2019	New policy format – policy better personalised to school
V 2.1	November 2019	Amalgamation of incident reporting form and incident record (Appendix E)
V 3.0	July 2020	Minor updates to new model policy and additional appendices including how to respond to negative social media
V 3.1.	July 2024	As per HCC guidelines (5.5.23) There is no statutory requirement for schools to have an Online Policy as the emphasis has moved toward fully integrating online safety across all school policies as relevant and substantially as part of the safeguarding policy.

BUILDING STRONG FOUNDATIONS FOR OUR CHILDREN

Batford Nursery School and Day Care, Holcroft Road, Harpenden AL5 5BQ

Batford Nursery School and Day Care is committed to:

- Safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment.
- Eliminating discrimination, advancing equality of opportunity and fostering good relations between different groups. These factors were considered in the formation and review of this policy and will be adhered to in its implementation and application across the whole school community.
- Promoting the fundamental British values of democracy, the rule of law, individual liberty and mutual respect and tolerance of those with different faiths and beliefs: any school member or visitor expressing opinions contrary to fundamental British Values, including 'extremist' views, will be actively challenged.

Contents

1.	Introduction	1
2.	Responsibilities	1
3.	Scope of policy	1
4.	Policy and procedure	2
4.1.	Use of email.....	2
4.2.	Visiting online sites and downloading.....	2
4.3.	Storage of Images	3
4.4.	Use of personal mobile devices (including phones)	3
4.5.	Reporting incidents, abuse and inappropriate material	4
5.	Curriculum	4
6.	Staff and Governor Training	4
7.	Working in Partnership with Parents/Carers.....	4
8.	Records, monitoring and review.....	5
Appendix A: Online Safety Acceptable Use Agreement – Staff, Governors, Student Teachers and Supply Staff		1
Appendix B: Requirements for visitors, volunteers and parent/carers helpers.....		3
Appendix C: Online safety policy guide		4
Appendix D: Guidance on the process for responding to cyberbullying incidents		5
Appendix E: Guidance for staff on preventing and responding to negative comments on social media		6
Appendix F- Online safety incident reporting form.....		7
Appendix G: Safeguarding and remote education during coronavirus (COVID-19).....		9

1. Introduction

Batford Nursery School recognises that internet, mobile and digital technologies provide positive opportunities for children to learn, socialise and play but they also need to understand 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 children in this setting will always require 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. The named online safety lead in this school is Sarah Hedges.

All breaches of this policy must be reported to Sarah Hedges.

All breaches of this policy that may have put a child at risk must also be reported to the DSL, Sarah Hedges or, in her absence, Laura Butler or Gemma Bacon.

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:

- teaching and support staff
- school governors
- peripatetic teachers/coaches, supply teachers, student teachers
- pupils
- parents/carers
- 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, behaviour, anti-bullying, Code of Conduct.

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 and strictly 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.

4.1. Use of email

Staff and governors should use a school email account for all official school communication, to ensure everyone is protected through the traceability of communication; emails to a school address must not be routinely forwarded to any other email address. Under no circumstances should staff contact parents or conduct any school business using a personal email address. Emails created or received as part of any school role will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000.

Staff, governors and pupils should not open emails or attachments from suspect sources and should report the receipt of any suspect messages to Sarah Hedges.

Users must not send emails which are offensive, embarrassing or upsetting to anyone (i.e. cyberbullying).

4.2. Visiting online sites and downloading

- Staff must preview sites, software and apps before their use in school or before recommending them to parents. Before using any online service that requires user accounts to be created or the sharing of any personal data, staff must consult with the Data Protection Officer with details of the site/service and seek approval from the Headteacher. The terms and conditions of the service should be read and adhered to. All users must observe copyright of materials from electronic sources.
- Staff must only use pre-approved systems if creating blogs, wikis or other online content.
- When working with pupils, searching for images should be done through Google Safe Search (standard through the HICS service), Google Advanced Search or a similar application that provides greater safety than a standard search engine.

Users must not:

- Visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:
 - Indecent images of children actually or apparently under the age of 18 or images of child abuse (i.e. images of children, digital or cartoons, involved in sexual activity or posed to be sexually provocative)
 - Indecent images of vulnerable people over the age of 18 (i.e. images of vulnerable people, digital or cartoons involved in sexual activity or posed to be sexually provocative)
 - Adult material that breaches the Obscene Publications Act in the UK
 - Promotion of discrimination of any kind in relation to the protected characteristics: age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race or ethnicity, religion or belief, sex, sexual orientation
 - Promotion of hatred against any individual or group from the protected characteristics above
 - Promotion of illegal acts including physical or sexual abuse of children or adults, violence, bomb making, drug and alcohol abuse and software piracy
 - Any material that may bring the school or any individual within it into disrepute e.g. promotion of violence, gambling, libel and disrespect

Users must not:

- Reveal or publicise confidential or proprietary information
- Intentionally interfere with the normal operation of the internet connection, including the propagation of computer viruses
- Transmit unsolicited commercial or advertising material either to other users, or to organisations connected to other networks except where permission has been given to the school
- Use the school's hardware or Wi-Fi facilities for running a private business
- Intimidate, threaten or cause harm to others
- Access or interfere in any way with other users' accounts
- Use software or hardware that has been prohibited by the school

All breaches of prohibited behaviours detailed above will be investigated, where appropriate, in liaison with the police.

4.3. 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. 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 network, on Tapestry and on the school's iPads; the photos stored to iPads are deleted or archived to the server at the end of each academic year.
- 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.

4.4. 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 only in the staff room and school offices and never in the presence of pupils. Only in emergency situations (e.g. during school closure or failure of telecommunication systems) does the school allow a member of staff to contact a parent/carer using their personal device – the 'withhold caller ID function' should be used.
- Parents/carers may not use personal mobile phones and devices within the school building unless otherwise informed, e.g. for specific events and activities. Phones should be switched off and out of sight whilst on the premises. Under no circumstance should images be taken at any time on school premises or on off-site school events and activities of anyone other than their own child, unless there is a pre-specified permission from Sarah Hedges.
- The school is not responsible for the loss, damage or theft on school premises of any personal mobile device that is brought onto the school site.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

- Where school business is conducted outside of school, e.g. via LARA or to access school emails from a personal mobile phone or other device, the device used must be password protected (or alternatively passwords must be entered to access the email via the internet page) and care should be taken to ensure that there is a locking function if there is no activity on the device for five minutes or more. The use of LARA (Login Anywhere Remote Access) – available to both staff and governors – avoids the need to download any school business documents onto personal machines.

4.5. Reporting incidents, abuse and inappropriate material

There may be occasions in school when a member of the school community receives an offensive, abusive or inappropriate message or accidentally accesses upsetting or abusive material. When such a situation occurs the recipient must report the incident immediately to the DSL, Sarah Hedges, or in her absence Laura Butler or Gemma Bacon. 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, the DSL will refer details to social care or the police.

5. Curriculum

Online safety, appropriate to the age of our pupils, is embedded within our curriculum.

Children are taught how to switch on the computer or iPad. Once a member of staff has logged on, the children are able to select an App or programme. The children are taught to ask an adult for help whenever they are unsure what to do.

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. We help the children to understand how to use the internet, mobile and digital technologies in a balanced and appropriate way to avoid negative impact on wellbeing, e.g. regulated screen time and diverse online activity.

6. Staff and Governor Training

Staff and governors are trained to fulfil their roles in online safety. The school audits the training needs of all school staff and provides regular training to improve their knowledge and expertise in the safe and appropriate use of internet, mobile and digital technologies. This training is recorded as part of safeguarding records.

New staff are provided with a copy of the online safety policy and must sign the school's Acceptable Use Agreement (Appendix A) as part of their induction and before having contact with pupils. This will be re-signed annually

Any organisation working with children and based on the school premises is also provided with a copy of the online safety policy and required to sign the Acceptable Use Agreement (Appendix A).

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 A)

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

Staff receive training on protecting their personal social media profiles, and guidance on how to respond to negative comments about the school or staff on social media (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.

It is important that parents/carers understand the crucial role they play in this process. The school seeks to regularly consult and discuss online safety with parents/carers and seeks to

promote a wide understanding of the benefits of new technologies and associated risks. The school provides regular updated online safety information through the school website, emails and newsletters and by other means.

A summary of key parent/carers responsibilities will also be provided and is available at Appendix C.

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 on CPOMS if related to a child or their family. All staff have the individual responsibility to ensure that incidents have been correctly recorded, acted upon and reported. An Online Safety Incident Reporting Form is provided at Appendix F

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, Student Teachers and Supply Staff

You must read this agreement in conjunction with the online safety policy and the Data Protection and Data Security policies. 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.

Introduction

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 Sarah Hedges. 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 the online safety lead 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.

I will report any accidental access to or receipt of inappropriate materials or filtering breach to Sarah Hedges.

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 the 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 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 on social networks. Where my school role is my only connection to an individual, private online contact with parents/carers is unacceptable.

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 post the name of my place of work (Hertfordshire County Council can be recorded as employer not the school directly).

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

Passwords

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

Data protection

I will follow requirements for data protection as outlined in the school's Data Protection and Data Security policies. These include:

- Photographs must be kept securely and used appropriately, whether in school, taken off the school premises or accessed remotely

- Personal data can only be taken out of school or accessed remotely when authorised by the headteacher or governing body
- Personal or sensitive data taken off site must be encrypted

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 by Sarah Hedges, Headteacher.

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 to receive and respond to all school business and will not forward my school emails to any other email address. 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 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 understand that the use of personal devices in school is at the discretion of the headteacher.

I will only use approved personal devices in designated areas and never in front of pupils.

I will not access secure school information from personal devices other than through LARA, which ensures any school documents accessed on a personal device remain on the school server and are never actually on the computer being used.

Additional hardware/software

I will not install any hardware or software on school equipment without permission of Sarah Hedges, Headteacher.

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 DSP or Sarah Hedges.

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.

Video conferencing

I will only use the conferencing tools that have been identified and risk by the Headteacher. The platform approved for general use is MS Teams. Zoom may also be used but only with the specific approval of the Headteacher.

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: Requirements for visitors, volunteers and parent/carers helpers

(Working directly with children or otherwise)

BATFORD NURSERY SCHOOL

Online safety lead: Sarah Hedges

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

I understand I may only use my personal mobile phone(s) and other devices with camera functions in the staff room or school offices. When not in a designated area, phones must be switched off and out of sight. Any exception must be pre-arranged.

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 parent/carers. Where appropriate I may share my professional contact details with parents/carers provided the 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 online, 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.

Signature

Date

Full Name
(please print)

Role

Appendix C: Online safety policy guide for parents

- Summary of key parent/carers 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 may only use personal mobile phones and devices in designated areas of the 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/carers is on school premises but not in a designated area, their phone/s must be switched off and out of sight.
- Parents/carers should not assume that pupils can bring technological devices to school and should always check the school policy.
- 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/carers, 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 D: 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 E: 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 C (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.

- Address 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 re-iterate the seriousness of the matter.

Appendix F- 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 **Part One** of 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 Sarah Hedges (Online Safety Lead).

PART ONE

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.

PART 2 (For completion by Online Safety Lead)

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)	
--	--

Name of person completing Part 2:	
Signature:	
Date actions completed:	

Appendix G: Safeguarding and remote education during coronavirus (COVID-19)

Useful resources

Below are resources (please note not an exhaustive list) to help schools manage and risk assess any remote teaching and working.

Government guidance on safeguarding and remote education

<https://www.gov.uk/guidance/safeguarding-and-remote-education-during-coronavirus-covid-19>

The Key for School Leaders- Remote learning: safeguarding pupils and staff

<https://schoolleaders.thekeysupport.com/covid-19/safeguard-and-support-pupils/safeguarding-while-teaching/remote-teaching-safeguarding-pupils-and-staff/?marker=content-body>

NSPCC Undertaking remote teaching safely

<https://learning.nspcc.org.uk/news/2020/march/undertaking-remote-teaching-safely>

LGfL Twenty safeguarding considerations for lesson livestreaming

<https://static.lgfl.net/LgflNet/downloads/digisafe/Safe-Lessons-by-Video-and-Livestream.pdf>

swgfl Remote working a guide for professionals

<https://swgfl.org.uk/assets/documents/educational-professionals-remote-working.pdf>

National Cyber Security Centre Video conferencing. Using services securely

https://www.ncsc.gov.uk/files/vtc_infographic.pdf