

This policy will be reviewed in full by the Senior Leadership Team on an annual basis.

Date the policy was last reviewed and agreed	SLT		SLT	
	Name	Signature	Name	Signature
January 2026	Natasha			

This policy is due for review up to 12 months from the above date

Safeguarding Children - Online Safety

CONTENTS

1	Introduction
2	Responsibilities
3	Scope of Policy
4	Policy and Procedure
5	Curriculum
6	Staff Training
7	Working in Partnership with Parents
8	Records, Monitoring, and Review
Appendix 1	Online Safety Acceptable Use Agreement – Staff
Appendix 2	Online Safety Acceptable Use Agreement - Peripatetic teachers/coaches, supply teachers, and Third Party Providers
Appendix 3	Requirements for visitors, volunteers and parent/carer helpers
Appendix 4	Online safety policy guide - Summary of key parent/carer responsibilities
Appendix 5	Guidance on the process for responding to cyberbullying incidents
Appendix 6	Guidance for staff on preventing and responding to negative comments on social media
Appendix 7	Online safety incident reporting form
Appendix 8	Online safety incident record
Appendix 9	Online safety incident log

Legal Basis: Related Sub Section in The Statutory Framework for The Early Years Foundation Stage (March 2021)

Child protection

3.4. Providers must be alert to any issues of concern in the child's life at home or elsewhere. Providers must have and implement a policy, and procedures, to safeguard children. These should be in line with the guidance and procedures of the relevant local safeguarding partners (LSP). The safeguarding policy and procedures must include an explanation of the action to be taken when there are safeguarding concerns about a child and in the event of an allegation being made against a member of staff, and cover the use of mobile phones and cameras in the setting. **To safeguard children and practitioners online, providers will find it helpful to refer to 'Safeguarding children and protecting professionals in early years settings: online safety considerations'**

1. INTRODUCTION

Our preschool recognises that internet, mobile and digital technologies provide positive opportunities for children and young people 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 children and staff 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

We have ultimate responsibility to ensure that appropriate online safety policy and practice is embedded and monitored. The named online safety lead in this preschool is Natasha Smyth.

All breaches of this policy must be reported to her. All breaches of this policy that may have put a child at risk must also be reported to the DSP.

3. SCOPE OF THE POLICY

The policy applies to:

- children
- parents/carers
- staff
- supply teachers, student teachers
- visitors
- volunteers
- voluntary, statutory or community organisations using the preschool's facilities

The preschool provides online safety information for parents/carers, for example, through the website, social media, in emails. 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 is linked to the following other preschool policies and documents: safeguarding, Keeping Children Safe in Education , GDPR, health and safety, behaviour, anti-bullying policies.

4. POLICY AND PROCEDURE

The preschool 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 preschool 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 preschool for children, parents/carers, staff and all other visitors to the preschool.

Use of email

Staff should use a preschool email account for all official preschool communication to ensure everyone is protected through the traceability of communication. Under no circumstances should staff contact parents or conduct any preschool business using a personal email address. For advice on emailing, sharing personal or confidential information or the need to gain parent permission refer to the policy for GDPR. Emails created or received as part of any preschool role will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000.

Staff should not open emails or attachments from suspicious sources and should report their receipt to Natasha Smyth.

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

Visiting online sites and downloading

- Staff must preview sites, software and apps before their use in preschool or before recommending them to families. 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 a senior manager. The terms and conditions of the service should be read and adhered to, and parental/carers permission sought where required. 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 children, searching for images should be done through Google Safe Search, 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
- Promoting 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
- Promoting hatred against any individual or group from the protected characteristics above
- Promoting 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 preschool 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 preschool
- Use the preschool's hardware and 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 preschool

Only a preschool device may be used to conduct preschool business outside of preschool. The only exception would be where a password protected external hard drive has been set up by the preschool for use on a personal device. The user must not save files locally to their own device, breaching data security.

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

The preschool recognises that in certain planned curricular activities, access to controversial and/or offensive online content may be beneficial for educational use. In such circumstances, there is an expectation that access is pre-planned, risk assessed and recorded, and permission given by Natasha Smyth.

Storage of Images

Photographs and videos provide valuable evidence of children's achievement and progress in a variety of contexts and can be used to celebrate the work of the preschool. In line with GDPR they are used only with the consent of parents/carers which is secured in the first instance on a child's entry to the preschool. Records are kept on file and consent can be changed by parents/carers at any time. (See GDPR policy for greater clarification).

Photographs and images of pupils are only stored on the preschool's phone and laptops. Rights of access to stored images are restricted to approved staff as determined by the manager. Staff may have temporary access to photographs taken during a session, but these will be transferred/deleted promptly.

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 preschool's Acceptable Use Agreement and refrain from taking or posting online photographs of any member of the preschool community, other than their own child/ren.

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

Use of personal mobile devices (including phones)

The preschool allows staff and visitors to use personal mobile phones and devices only in designated areas and never in the presence of children. Under no circumstance (except in an emergency) does the preschool allow a member of staff to contact a child or parent/carer using their personal device.

The preschool is not responsible for the loss, damage or theft of any personal mobile device that is brought into preschool.

Users bringing personal devices into preschool must ensure there is no inappropriate or illegal content on the device.

Personal mobiles must never be used to access preschool emails and data.

New technological devices

New personal technological devices may offer opportunities for teaching and learning. However, the preschool must consider educational benefit and carry out risk assessment before use in preschool is allowed. Parents/carers, children and staff should not assume that new technological devices will be allowed in preschool and should check with the manager before they are brought into preschool.

Reporting incidents, abuse and inappropriate material

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

5. CURRICULUM

The preschool provides an age appropriate curriculum for online safety which enables children to be safe. The curriculum is flexible and can respond to any immediate online safety issues and risks as they emerge.

6. STAFF TRAINING

Staff are trained to fulfil their roles in online safety. The preschool audits the training needs of all preschool 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 as part of their induction and before having contact with pupils.

Students and regular visitors are provided with a copy of the online safety policy and are required to sign the Acceptable Use Agreement (Appendix 2). Guidance is provided for occasional visitors, volunteers and parent/carer helpers.

7. WORKING IN PARTNERSHIP WITH PARENTS/CARERS

The preschool works closely with families to help ensure that children can use internet, mobile and digital technologies safely and responsibly both at home and preschool. 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 preschool 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.

8. STEPS BEHAVIOUR MANAGEMENT STRATEGY

The preschool 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 children 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 preschool supports children 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 preschool's behaviour and disciplinary policies as appropriate. Breaches may also lead to criminal or civil proceedings.

STAFF DECLARATION

I agree that I have read and understood the information set out in this policy, and will abide by it. I understand that if I have any questions about this policy, I will raise them with my manager prior to signing my agreement below.

Staff Name	Staff Signature	Date

APPENDIX 1: ONLINE SAFETY ACCEPTABLE USE AGREEMENT - 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 preschool. 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 are aware of their responsibilities in relation to their use. All staff are expected to adhere to this agreement and to the online safety policy. Any concerns or clarification should be discussed with the Manager. 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 preschool equipment must be treated as an online safety incident, reported to the online safety lead and/or DSP and an incident report completed.

Online conduct

I will ensure that my online activity, both in and outside preschool, will not bring the preschool, 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 the Manager.

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 manager 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 & social media

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 preschool 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 preschool, its staff, parents/carers or children. Privileged information must remain confidential.

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

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 GDPR policy. These include:

- Photographs must be kept securely and used appropriately, whether in preschool, taken off the preschool premises or accessed remotely
- Personal data can only be taken out of preschool or accessed remotely when authorised by the senior manager
- Personal or sensitive data taken off site must be password protected

Images and videos

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

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

Use of email

I will use my preschool email address (if applicable) for all preschool 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 preschool email addresses for personal matters or non-preschool 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 preschool is at the discretion of the senior manager.

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

I will not access secure preschool information from personal devices when in preschool or any other location. Saving files locally to my own device is a breach of data security.

Additional hardware/software

I will not install any hardware or software on preschool equipment without permission of the manager.

Promoting online safety

I understand that online safety is the responsibility of all staff and I will promote positive online safety messages at all times.

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

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 children. I will also check the appropriateness of any suggested sites suggested for home learning.

If I am using the internet to teach about controversial issues I will secure, on every occasion, approval in advance for the material I plan to use with the senior manager.

Video conferencing

I will only use the conferencing tools that have been identified and risk assessed by the preschool leadership or DSP. A preschool-owned device should be used when running video-conferences, where possible.

User signature

I agree to follow this Acceptable Use Agreement and to support online safety throughout the preschool. 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 volunteer.

Signature Date

Full Name (printed)

Job title

APPENDIX 2: ONLINE SAFETY ACCEPTABLE USE AGREEMENT – SUPPLY STAFF & THIRD PARTY ACTIVITY PROVIDERS

Preschool Name:

Online safety lead:

Designated Safeguarding Lead (DSP):

This agreement forms part of your professional and safeguarding responsibility in the preschool. 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 volunteers 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 the manager. Breaches will be investigated, recorded and, where appropriate, disciplinary procedures will apply and police involvement will be sought.

The preschool'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 preschool equipment must be treated as an online safety incident, reported to the online safety lead and/or DSP and an incident report completed.

Online conduct

I will ensure that my online activity, both in and outside preschool, will not bring the preschool, 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 the DSP.

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 manager 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.

Should I need to share my professional details, such as mobile phone number or email address, with parent/carers, this must be agreed in advance as an acceptable approach with the manager.

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 preschool role is my only connection to an individual, private online contact is unacceptable with parents/carers or pupils.

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

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

Passwords

I must clarify what access I may have to the internet and/or preschool systems. If I have access of any kind, 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 all requirements for data protection explained to me by the preschool. These include:

- I must consult with the preschool before making any recordings, photographs and videos. Once agreed, these must be made on a preschool 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 only upload images or videos of staff, children or parents/carers onto preschool approved sites where specific permission has been granted.

I will not take images, sound recordings or videos of activities on any personal device. Preschool devices can be used for this purpose or. Recordings can be made with the parent/carer's agreement on a preschool device.

Use of Email

I will only use my professional email address for all preschool 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 preschool 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 preschool is at the discretion of the manager.

I will only use approved personal devices in designated areas and never in front of children. This therefore precludes use of specialist apps on personal devices. A preschool device could be used to access specialist apps that support child learning.

Additional hardware/software

I will not install any hardware or software on preschool equipment without permission of the manager.

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 preschool safeguarding approach and will report any behaviour (of staff, visitors, children or parents/carers) which I believe may be inappropriate or concerning in any way to the DSP.

Classroom management of internet access

I will pre-check for appropriateness all internet sites used in the classroom or during a tutoring session; 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.

If I am using the internet to teach about controversial issues I will secure, on every occasion, approval in advance for the material I plan to use with manager.

Video conferencing

I will only use the conferencing tools that have been identified and risk assessed by the preschool leadership and DSP. A preschool-owned device should be used when running video-conferences, where possible

User Signature

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

Signature Date

Full Name (Please use block capitals)

Job Title/Role

APPENDIX 3: REQUIREMENTS FOR VISITORS, VOLUNTEERS AND PARENT/CARER HELPERS (WORKING DIRECTLY WITH CHILDREN OR OTHERWISE)

Preschool name.....

Online safety lead

DSP

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

Please raise any safeguarding concerns arising from your visit immediately with the manager and/or DSP

- I understand I may only use my personal mobile phone(s) and other devices with camera functions in designated areas. 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 preschool 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 without first consulting the manager before I leave the preschool.
- I understand my visit to the preschool may give me access to privileged information about pupils, staff, preschool systems and plans. Such information should never be shared on line, including on social media sites.
- I understand I should not use preschool equipment to access the internet without prior approval from my contact in the preschool or the manager.
- 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 preschool.

User Signature

I agree to follow this Acceptable Use Agreement and to support online safety in my work in the preschool

Signature Date

Full Name (Please use block capitals)

Job Title/Role

APPENDIX 4 - 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 how to stay safe online.
- 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/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 5 - 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 6 - 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 re-iterate the seriousness of the matter.

APPENDIX 7 - 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 manager.

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 8 - 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 manager/DSP	
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 9 - ONLINE SAFETY INCIDENT LOG

Summary details of ALL online safety incidents will be recorded on this form by the DSL 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