



At Chellaston Infant School, we believe that everyone should reach their full potential in a safe, fun and happy environment which promotes independence, self-worth and excellence. Everyone is a learner whose values are respected.

Chellaston Infant School  
 School Lane, Chellaston  
 DERBY, DE73 6TA  
 Telephone: 01332 700298

Email: [admin@chellastoni.derby.sch.uk](mailto:admin@chellastoni.derby.sch.uk)  
 Website: [www.chellastoninfants.co.uk](http://www.chellastoninfants.co.uk)

**Headteacher:** Lindsay Galley

## ONLINE SAFETY POLICY

Date	Change made where?	Change description	Approved by Governors	Next review
18.10.21		New policy to better reflect new Computing scheme of work and safeguarding practices in school.	<b>Autumn 1 2021</b>	<b>Autumn 1 2022</b>

### Contents

ONLINE SAFETY POLICY .....	1
Introduction .....	2
Legislation and guidance.....	2
Roles and responsibilities.....	2
Educating pupils about online safety .....	4
Educating parents about online safety .....	7
Cyber-bullying .....	7
Acceptable use of the internet in school .....	7
Staff using work devices outside school .....	8
Photographs.....	8
Social Media .....	8
How the school will respond to issues of misuse .....	8
Training .....	8
Monitoring arrangements.....	9
Links with other policies .....	9
COVID-19 and home learning .....	9

## Introduction

The amount of people connected to the internet is increasing daily (SWGfL). Technology is advancing and providing an ever-increasing range of methods to access the internet. At Chellaston Infant School we recognise the increasing prominence of technology and the internet in daily life. We endeavour to empower our pupils to be confident users of technology and the internet, being able to identify ways to be safe online and who they can talk to if they have any concerns or worries. To enable this, we aim to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

## Legislation and guidance

This policy is underpinned by the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships education and health education

It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010.

The policy also takes into account the National Curriculum computing programmes of study.

This policy complies with our funding agreement and articles of association.

This policy also complies and links to the EMET Employee Code of Conduct with regards to photography and social media.

## Roles and responsibilities

Online Safety Leaders in school:

- Lindsay Galley: Designated Safeguarding Lead
- Lynn Hateley: Deputy Designated Safeguarding Lead
- Rachel Leyland: Deputy Designated Safeguarding Lead
- Kelly Leader: Learning Mentor & member of the Safeguarding Team
- Joseph Jeffery: Computing Lead
- Paul Stevenson: Safeguarding Lead Governor
- Mark Faulkner: ICT manager (based at QEGS Multi Academy Trust)

## The Governing Board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs on CPOMS as provided by the designated safeguarding lead (DSL).

The governors responsible for safeguarding will also oversee online safety.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2).

## **Lindsay Galley – Headteacher and Designated Safeguarding Lead**

Lindsay Galley is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school, as underpinned by the Keeping Children Safe in Education guidance. The headteacher/DSL will be alerted to any Online Safety concerns logged through CPOMS along with the school's safeguarding team.

The Headteacher/DSL takes lead responsibility for online safety in school, in particular:

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged through CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and providing staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the governing board and computing lead to enable any concerns to be taught in online safety lessons

This list is not intended to be exhaustive.

## **Mark Faulkner - ICT manager**

The ICT manager is responsible for:

- Putting in place appropriate filtering and monitoring systems (see Appropriate Monitoring and Filtering Procedures), which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems frequently
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

This list is not intended to be exhaustive.

## **Joseph Jeffery – Computing Lead**

- Ensure that online safety lessons are planned and delivered across school
- Ensure that staff are confident with their online safety subject knowledge and provide CPD with the headteacher
- Ensure that any concerns with technology used in school are reported to the ICT manager to be swiftly resolved
- Updating the online safety policy with the headteacher to reflect the computing curriculum.

## **All staff and volunteers**

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently.
- Class based staff to teach online safety lessons.
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2).
- Class staff to produce an acceptable use policy with the children at the start of each academic year to provide ownership and understanding for pupils.
- Working with the DSL to ensure that any online safety incidents are logged through CPOMS and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.

› This list is not intended to be exhaustive.

## Parents

Parents are expected to:

- › Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- › Ensure the Acceptable Use Policy has been read and agreed

## Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

## Educating pupils about online safety

The teaching of online safety is a paramount aspect of our computing curriculum. We use the Project Evolve: Education for a Connected World. Online safety lessons are taught every term, starting with each class creating an acceptable use policy that each pupil will receive a copy of for their work folders. The strands taught through the scheme are:

- Online bullying
- Online relationships
- Copyright and ownership
- Self-image and identity
- Privacy and security
- Managing online information
- Online reputation
- Health, well-being and lifestyle

The online safety scheme links to the following National Curriculum objectives:

- › Use technology safely and respectfully, keeping personal information private
- › Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

The teaching of online safety is a cross-curricular subject, with staff making links where appropriate to other subjects in the school curriculum.

Through online safety lessons and assemblies, staff will raise pupils' awareness of the dangers that can be encountered online by teaching the children how to be safe online. The school celebrate online safety events, such as Safer Internet Day and Anti-Bullying Week to promote online safety. Staff adapt teaching to current online safety issues such as new applications or software the children may access inside or outside of school.

Some of the key vocabulary that the children will learn and use are:

- Share
- Personal information
- Online safety
- Private/privacy
- Online
- Data
- Identity
- Reputation
- Online bullying
- Copyright
- Social media

	Aut 1	Aut 2	Spring 1	Spring 2	Summer 1	Summer 2
FS	<p><b>Technology All Around Us: Introduction to using the devices in school.</b></p> <p>Online Safety Create an Acceptable Use Policy in each class.</p>	<p><b>Programming – sequencing using unplugged activities</b></p> <p>Link to debugging</p> <p>Online Safety Online bullying</p>	<p><b>Digital Creators: Using Draw and Tell app to create a picture and record what they have made.</b></p> <p>Online Safety Online relationships</p>	<p><b>Digital Creators: Online Safety Copyright and ownership</b></p>	<p><b>Programming – sequencing using unplugged activities</b></p> <p>Link to debugging</p> <p>Online Safety Self-image and identity</p>	<p><b>Opportunities to practise any skills the children have found tricky/not yet covered.</b></p> <p>Online Safety Privacy and security</p> <p>Managing online information</p>
Y1	<p><b>Technology All Around Us: Parts of a computer. What this looks like in real world</b></p> <p>Online Safety Create an Acceptable Use Policy in each class.</p>	<p><b>Programming – understanding and creating algorithms unplugged and beebot activities.</b></p> <p>Link to debugging</p> <p>Online Safety Online bullying</p>	<p><b>Digital Creators: Digital art – using iPad to create and edit a picture</b></p> <p>Online Safety Online relationships</p>	<p><b>Data handling: Using websites and apps to sort and classify objects by their properties</b></p> <p>Online Safety Copyright and ownership</p>	<p><b>Programming with Scratch Jr. Exploring the app and the different elements.</b></p> <p>Online Safety Self-image and identity</p>	<p><b>Opportunities to practise any skills the children have found tricky/not yet covered.</b></p> <p>Online Safety Privacy and security</p> <p>Managing online information</p>
Y2	<p><b>Technology All Around Us: Parts of a computer – understanding how they work What this looks like in real world</b></p> <p>Online Safety Create an Acceptable Use Policy in each class.</p>	<p><b>Programming – Scratch Jr</b></p> <p>Link to debugging</p> <p>Online Safety Online bullying</p>	<p><b>Digital Creators: Stop Motion Animation</b></p> <p>Online Safety Online relationships</p>	<p><b>Data handling Using Purple Mash to create pictograms. Databases</b></p> <p>Online Safety Copyright and ownership</p>	<p><b>Programming with Scratch Jr. Designing and programming.</b></p> <p>Online Safety Self-image and identity</p>	<p><b>Opportunities to practise any skills the children have found tricky/not yet covered.</b></p> <p>Online Safety Privacy and security</p> <p>Managing online information</p>

This is our long term plan for computing. The green strands are the online safety aspects of the computing curriculum. Online Reputation and Health, Well-being and Lifestyle strands from the scheme will be delivered through school assemblies.

Online Safety Overview Project Evolve – Educated for a Connected World			
	Foundation Stage	Year 1	Year 2
Self-image and identity	In this strand children will learn how to say no to people when online and in real life using different scenarios and discuss what the appropriate thing to do is.	In year 1 children will learn how to recognise how people may be feeling online and who to talk to if they are worried about being online.	In year 2 children will learn how people may act differently online and offline and learn some different issues people may encounter that may make them sad or upset.
Online relationships	In FS2 the children will begin to understand how the internet can be used to communicate with other people.	In year 1 children will learn the importance of asking for permission before accessing the internet. Children will discuss examples of how they have used the internet to connect with others such as video calls. They will learn the importance of kindness to others when communicating online.	In year 2 the children will develop their understanding of asking for permission before agreeing/doing something online by asking a trusted adult. Children will be able to identify who their trusted adults are at home and in school.
Online reputation	Children will begin to learn how information can be put online.	Children in year 1 will learn that information put online can stay there for a long time and be copied by other people. Children will develop their understanding of what information is safe for them to put online and the necessity for them to check with a trusted adult first.	The children will learn about their digital footprint and how information that is put on the internet is very hard to permanently remove. They will learn that information that they put online can be viewed by other people.
Online bullying	Children will learn how people can be unkind online and be able to explain how this might make people feel.	In year 1 children will explore how to behave online so that they do not upset other people.	Children will learn to explain what online bullying is, that anyone who experiences bullying is not to blame and how and who to go to for help if being bullied online.
Managing online information	Children will begin to learn how the internet can be used as a source to find information. Children will discuss the different devices that they could use to access the internet.	Children will learn the different ways that they can use tools to search for information on the web. They will learn that not everything that they read or see on the internet is real and what to do if they see something that upsets or worries them online.	Children will learn how to search for information with key words, how to navigate a webpage, understand what voice activated searching is and understand that not everything on the internet is true.
Health, well-being and lifestyle	Children will learn how to be safe and healthy when using technology at home and beyond home.	The children will learn to express how to be safe when using technology at home or beyond home.	The children will learn how to explain the rules and guidance for using different technology in school, home and public places and how these rules help people accessing online technologies.
Privacy and security	Children will begin to understand what information is personal and who are trusted people that information can be shared with.	Children will learn about the importance of passwords and the information that is personal to ourselves. They will learn of the importance to ask a trusted adult before sharing information online.	Children will continue to learn about passwords, what keeping information private means, be able to explain how they can keep their information private and understand what devices are connected to the internet in their homes.
Copyright and ownership	Children will begin to understand that the work they create belongs to them.	Children will develop their understanding that the work they create belongs to them and that things other people have created do not belong to them.	Children will continue to develop their understanding that work produced by them belongs to them and that things created by others does not belong to them.

This is the long term overview of our online safety curriculum that follows the Education for a Connected World scheme.

## **Educating parents about online safety**

The school will raise parents' awareness of online safety in newsletters and in information via our website or Class Dojo. This policy will also be shared with parents via the school website. Training from external trainers have previously been offered for parents and carers.

Online safety will also be covered during parents' evenings as appropriate.

If parents have any queries or concerns in relation to online safety, these can be raised to any member of staff who will ensure that the headteacher and the safeguarding team are informed.

Concerns or queries about this policy can be raised with any member of staff who will inform the headteacher and the computing lead.

## **Cyber-bullying**

### **Definition**

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

### **Preventing and addressing cyber-bullying**

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. This will be more specifically taught through the Online Bullying strand of the Project Evolve: Education for a Connected World scheme.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also provides information on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material and will work with external services if it is deemed necessary to do so.

## **Acceptable use of the internet in school**

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1, 2 and 3)

Pupils will create an acceptable use policy with their class teachers each year in Autumn 1 that is referred to throughout the year when appropriate (appendix 1).

Visitors will be expected to read and agree to the school's terms on ICT and Internet acceptable use as established in this policy if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

When using email or electronic communications involving pupil information, staff will use initials or first names only to ensure that personal information is protected.

More information is set out in the acceptable use agreements in the appendices.

## **Staff using work devices outside school**

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2.

Staff laptops are secured with Bitlocker passcodes. Staff also have their own login details that they can use. School tablets are also password protected. Staff must not share their passwords with anyone not authorised to use the school devices. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted. If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

Staff are permitted to occasionally use school ICT facilities for personal use subject to certain conditions set in the ICT and Internet Acceptable Use Policy. Personal use of ICT facilities must not be overused or abused. The School IT team may withdraw permission for it at any time or restrict access at their discretion.

## **Photographs**

*Taken from the EMET Employee Code of Conduct:*

If there is a requirement in the member of staff's role to take photographs of children for school purposes this must be carried out using school equipment. Any photographs taken in school remain the property of the school and will only be used for official school business such as displays, the school web site or newsletters. No images taken within the school premises should be published unofficially by individuals on social media or other such forums.

## **Social Media**

*Taken from the EMET Employee Code of Conduct:*

Staff should be extremely cautious when using social media or networking sites outside of work and avoid publishing, or allowing to be published, any material, including comments or images that could damage their professional reputation and/or bring their school or the Trust into disrepute. Where staff do use social media or networking sites, profiles should be set as 'private' and under no circumstances should staff allow access to pupils, their families or carers.

Staff and governors should be mindful that requirements in relation to maintaining the confidentiality of pupils, their families, colleagues and any matters relating to the school itself apply to all forms of communication, including social media and networking sites.

## **How the school will respond to issues of misuse**

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and ICT and internet acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate. If appropriate, staff will log any concerns on CPOMS so that the safeguarding team is aware of the issue, as well as the computing lead if the issue involves resources used for computing and online safety lessons.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident. The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

## **Training**

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation. All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, briefings and staff meetings).

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals,

and at least annually. Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Staff teaching online safety lessons will have training to ensure lessons are taught effectively, which will be monitored through learning walks, observations and planning/work scrutinies. Staff will regularly complete a skills audit for online safety that can be used by the computing lead and headteacher to plan and provide CPD where necessary (appendix 4).

Volunteers will receive appropriate training and updates, if applicable. More information about safeguarding training is set out in our child protection and safeguarding policy.

## Monitoring arrangements

All staff will log behaviour and safeguarding issues related to online safety. Any incident should be logged on CPOMS and the safeguarding team made aware. Visitors will report any concerns to a member of staff so that the concern can be correctly logged on CPOMS. Any concerns that become repetitive across school may be alerted to the computing lead so that online safety lessons/assemblies can be taught to address these concerns if appropriate. This policy will be reviewed every year by the computing team. At every review, the policy will be shared with the governing board.

Monitoring and filtering of the school's wi-fi is managed by Mark Falkner and QEGS Multi Academy Trust. For more information see the Monitoring and Filtering Procedures policy.

## Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
  - Behaviour policy
  - Staff disciplinary procedures
  - Data protection policy and privacy notices
  - Complaints procedure
  - Appropriate Monitoring and Filtering Procedures
- Acceptable Use Policy

## COVID-19 and home learning

Due to COVID-19 learning has occurred from home for many children during past few academic years. Staff have provided resources and activities for parents and carers to use for home learning. All websites and resources provided are rigorously checked by staff before being shared to ensure that there is no inappropriate content that the children may access. Photos uploaded onto the children's portfolios on Class Dojo were approved by staff to ensure that content is appropriate.

In the current 2021-2022 academic year, home learning will be provided if there is a partial or full school closure. Home learning will be posted onto the school website and a link will be shared with parents when necessary. Class Dojo will continue to be used as a method of communication between staff and parents/pupils. Loom has also been used by staff to provide educational videos to support the curriculum content provided through home learning. Videos are checked by staff to ensure that all content is appropriate for children to watch at home.

Children will be given the opportunity for daily contact with staff through submitting work onto their Class Dojo portfolios which is acknowledged and feedback given by class staff. When delivering video assemblies or teaching with Zoom and/or Loom, staff will ensure that they are in a suitable environment while using any webcam to ensure secure and safe broadcasts. Any non-engagement with home learning will initially be followed up by the class teacher through a supportive conversation with parents or carers. SLT will provide further support if necessary.

We will:

- Check parents and carers access to the internet, devices and the number of these at home etc. along with their comments on the home learning when appropriate.
- Remind parents of the risks of using online resources and provide support and resources where appropriate to keep the children safe.

## Useful Links and Resources

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? - [UK Safer Internet Centre](#)
- <https://www.childnet.com/parents-and-carers/hot-topics>
- Parent resources document - <https://www.childnet.com/resources/parents-and-carers-resource-sheet>
- This website reviews different games/apps and their safety features and risks <https://www.net-aware.org.uk/>
- Our school online safety webpage <https://www.chellastoni.derby.sch.uk/about-us/online-safety/>
- National Online Safety Website - <https://nationalonlinesafety.com/>
- Keeping Children Safe in Education - <https://www.gov.uk/government/publications/keeping-children-safe-in-education--2>
- Teaching Online Safety in Schools - <https://www.gov.uk/government/publications/teaching-online-safety-in-schools>
- Think U Know – online safety resources for children - <https://www.thinkuknow.co.uk/professionals/>
- Education for a Connected World - [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/896323/UKCIS\\_Education\\_for\\_a\\_Connected\\_World\\_.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/896323/UKCIS_Education_for_a_Connected_World_.pdf)

## Appendix

**Appendix 1 – Acceptable Use Policy - class/children**

**Appendix 2 – Acceptable Use Policy – Staff, Governors, Volunteers and Visitors**

**Appendix 3 – Acceptable Use Policy – Parents and Carers**

**Appendix 4 – Online Safety Staff Training Needs Audit**

## Appendix 1

### Acceptable Use Policy – Class/Children



#### Keeping Safe Online and Computing Rules

#### By Class

**This is how we stay safe when we are using computers:**

Written and agreed by Class

## Appendix 2

### Acceptable Use Policy – Staff, Governors, Volunteers and Visitors

#### ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS

**Name of staff member/governor/volunteer/visitor:**

**When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:**

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Take photographs of pupils without checking with teachers first
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) know if a pupil informs me they have found any material which might upset, distress or harm them or others via CPOMS, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

**Signed (staff member/governor/volunteer/visitor):**

**Date:**

## Appendix 3

### Acceptable Use Policy – parents and carers

#### ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PARENTS/CARERS

**Name of Parent/carers:**

**When I use any ICT systems for working/communication with school:**

- Use content shared on Class Dojo and the school website appropriately.
- Keep photos shared on Class Dojo and the school website private and not share them on social media.
- Keep any passwords for accounts for websites provided by school private.
- Communicate in an appropriate and respectful manner.
- Ensure any concerns regarding online safety are shared with the school.
- Ensure any content shared via school communication systems (e.g. Class Dojo, email) is appropriate and safe.
- Use social media respectfully in relation to school, share any concerns with staff.
- I will not use any devices to record or photograph children at school events.

**Parent/carer agreement:** I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for working and communicating with the school's ICT systems

**Signed (parent/carer):**

**Date:**

## Appendix 4

### Online Safety Training Needs Audit

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	Date:
Question	Yes/No (add comments if necessary)
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for parents?	
Are you familiar with the school's acceptable use agreement for children?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	