Crown Meadow First School and Nursery

Online Safety Policy

This policy is reviewed at least annually by the governing body and SLT and was

Last reviewed on Date: April 2025

Next Review Date: April 2028

Print Name: Tess Davis **Signature**
(Chair of Governors)

Print Name: Michelle Hague **Signature:**
(Head Teacher)

AIMS:

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, including mobile and smart technology.
Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

CMFS Online Safety Policy

The 4 key categories of risk
Our approach to online safety is based on addressing the following categories of risk:

Content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories.

Contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

Conduct: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and

Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

Legislation and guidance

This policy is based on the Department for Education's (DfE's) 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 and Searching, screening and confiscation It also refers to the DfE'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. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so. The policy also takes into account the National Curriculum computing programmes of study.

Roles and responsibilities

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 as provided by the designated safeguarding lead (DSL).
The governor who oversees online safety is the safeguarding governor.

All governors will:
Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet.
Ensure that online safety is a running and interrelated theme while devising and implementing their whole school or college approach to safeguarding and related policies and/or procedures.
Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

CMFS Online Safety Policy

The headteacher / The designated safeguarding lead

Responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school

Working with the IT manager and other staff, as necessary, to address any online safety issues or incidents.

Managing all online safety issues and incidents in line with the school child protection policy.

Ensuring that any online safety incidents are logged 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 delivering 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 headteacher and/or governing board.

To view and respond to flags of incidents captured by the monitoring and filtering system Securus on the day that they arise and to report on the security protection systems to governors at least termly.

The IT manager - Entrust

The ICT manager is responsible for:

Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept 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.

Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.

Shortcomings in the infrastructure are reported to the head teacher so that appropriate action may be taken.

All staff and volunteers

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

Maintaining an understanding of this policy.

Implementing this policy consistently.

Agreeing and adhering to the terms on acceptable use of the school's IT systems and the internet, and ensuring that pupils follow the school's terms on acceptable use.

Working with the DSL to ensure that any online safety incidents are logged 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.

Responding appropriately to all reports and concerns about child on child abuse, both online and offline and maintaining an attitude of 'it could happen here'.

CMFS Online Safety Policy

Parents

Parents are expected to:

Notify a member of staff or the headteacher of any concerns or queries regarding this policy.

Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet in their communication book.

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

What are the issues? – UK Safer Internet Centre

Hot topics – Childnet International

Parent resource sheet – Childnet International

How to report= Internet Watch Foundation

Parental Guidance for different age pupils = ThinkuKnow

Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

The text below is taken from the National Curriculum computing programmes of study.

It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

All schools are required to teach:

Relationships education and health education in primary schools

In **Key Stage 1**, pupils will be taught to:

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.

Pupils in **Key Stage 2** will be taught to:

Use technology safely, respectfully and responsibly.

Recognise acceptable and unacceptable behaviour.

Identify a range of ways to report concerns about content and contact.

By the **end of primary school**, pupils will know:

That people sometimes behave differently online, including by pretending to be someone they are not.

That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous.

The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them.

How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met.

How information and data is shared and used online.

What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context).

How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.

Cross curricular links - The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

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 1 person or group by another person or group, where the relationship involves an imbalance of power.

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.

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 have received training on cyber-bullying, its impact and ways to support pupil.

The school also sends information on the newsletter where necessary to highlight concerns to parents.

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 report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

Acceptable use of the internet in school

All pupils and staff are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet.

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 and staff to ensure they comply with the above.

Staff may use the internet for personal use but will be held to professional standards and staff code of conduct.

See Appendix 1

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 behaviour policies and acceptable use agreement. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

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 disciplinary procedures. 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.

See flow chart Appendix 2

CMFS Online Safety Policy

Pupils bringing mobile devices into school

Pupils are strongly discouraged from bringing mobile devices into school due to their age groups of pupils. If by agreement a device is brought into school, it will be handed into the office at the start of the day and be collected at the end of the day by a parent.

Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain out of reach of children at all times and no children are in the vicinity, or likely to be. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drives are encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the devices are locked if left inactive for a period of time
- Not permitting friends or family to use a devise belonging to school
- Ensuring that laptops are regularly brought into school for latest update installation.
- Staff members must use the device for the purposes of school only and never in any way which would violate the school's terms of acceptable use, which is annually renewed and signed by staff.

Appendix 3 – Staff and Pupil use of technology charts

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 and staff briefings).

By way of this training, all staff will be made aware that:

Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse

Children can abuse their peers online through:

- Abusive, harassing, and misogynistic messages.
- Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups .
- Sharing of abusive images and pornography, to those who don't want to receive such content.
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element.

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse.
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks.
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term
- More information about safeguarding training is set out in our child protection and safeguarding policy.

Monitoring arrangements

The DSLs logs behaviour and safeguarding issues related to online safety on CPOMS.

CMFS Online Safety Policy

Whole School approach and Links with other policies

i) Core ICT policies

Computing statement	How computing is used, managed, resources and supported in out school
Online safety Policy	How we strive to ensure that all individuals in school stay safe while using Learning Technologies. The online safety policy constitutes a part of the computing statement and draws on training from 'Prevent' and cyberbullying.
School Systems and Data Protection Policy	How we categorise, store and transfer sensitive and personal data and protect systems. This links strongly and overlaps with the online safety policy.
Computing curriculum (CUSP)	Key documents and associated resources directly relating to learning covering the Computing Curriculum

ii) Other policies relating to online safety

Anti-bullying	How your school strives to eliminate bullying - link to cyber bullying
PSHE	Online safety has links to staying safe
Safeguarding	Safeguarding pupils electronically is an important aspect of Online safety. ***The online safety policy forms a part of the school's safeguarding policy***
Behaviour	Positive strategies for encouraging online safety and sanctions for disregarding it
Peer on Peer Abuse	How school strives to keep children safe at school and online
Use of images	WCC guidance to support the safe and appropriate use of images in schools, academies and settings
Staff disciplinary procedures	
Data protection policy and privacy not	
Complaints procedure	
Acceptable use agreement	

Policy Review

This policy will be reviewed every three years or sooner if it is considered necessary as linked policies are updated.

CMFS Online Safety Policy

APPENDIX 1 – Acceptable Use Agreement

Acceptable use of the school's ICT systems and internet: Agreement for pupils

Name of pupil:

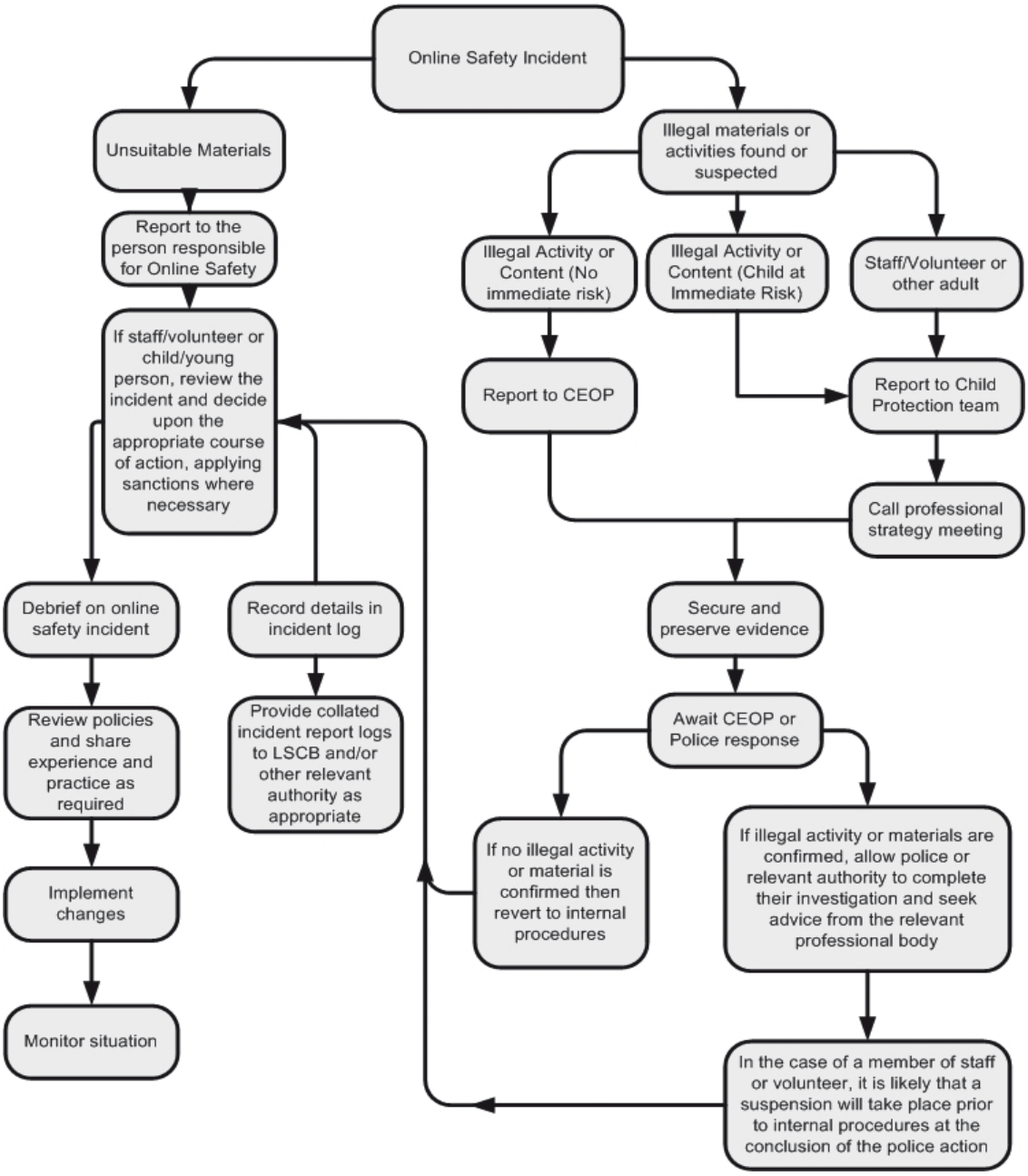
When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Ask a teacher or adult if I can do so before using them.
- Only use websites that a teacher or adult has told me or allowed me to use.
- Tell my teacher immediately if:
    - I click on a website by mistake.
    - I receive messages from people I don't know.
    - I find anything that may upset or harm me or my friends.
- Use school computers for school work only.
- Be kind to others and not upset or be rude to them.
- Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly.
- Only use the username and password I have been given.
- Try my hardest to remember an issued username and password
- Never share my password with anyone, including my friends
- Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
- Save my work on the school network when appropriate.
- Check with my teacher before I print anything.
- Log off or shut down a computer when I have finished using it.

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (pupil): **Date:**

APPENDIX 2 – How school responds to issues of misuse



APPENDIX 3 – Staff and Pupil use of technology charts

3.1 Personal hand held technology *It is important that schools/academies review this table in the light of principles agreed within their own establishment.*	Staff / adults				Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones / smart watches may be brought into the school	✔							✔
Use of mobile phones/smart watches in lessons				✔				✔
Use of mobile phones/smart watches in social time		✔						✔
Taking photos on personal phones or other camera devices				✔				✔
Use of hand held devices e.g. PDAs, gaming consoles		✔					✔	

3.2 Use of Email *It is important that schools/academies review this table in the light of principles agreed within their own establishment.*	Staff / adults				Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Use of personal email accounts in school / on school network		✔						✔
Use of school email for personal emails				✔				✔

3.3 Use of social networking tools *It is important that schools/academies review this table in the light of principles agreed within their own establishment.*	Staff / adults				Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Use of non-educational chat rooms etc.		✔						✔
Use of non-educational instant messaging		✔						✔
Use of non-educational social networking sites		✔						✔
Use of non-educational blogs		✔						✔