Worlingham CEVC Primary School

ICT AND ONLINE SAFETY POLICY

Due consideration has been given to all children/adults/stakeholders with regard to the protected characteristics under the Equality Act 2010.

Date approved:	17.11.2026
Name of Committee:	Full Governing Body
Chair of Committee signature:	*Mr Mark Hurren*
Date of next review:	Autumn 2027

Headteacher: Mrs Holly Marchand
School No. 935 3111

Worlingham CEVC Primary School

ICT AND ONLINE SAFETY POLICY

Contents

1. Aims.....
2. Legislation and guidance.....
3. Roles and responsibilities.....
4. Educating pupils about online safety.....
5. Educating parents about online safety.....
6. Cyber-bullying.....
7. Acceptable use of the internet in school.....
8. Pupils using mobile devices in school.....
9. Bring Your Own Device Policy.....
9.1 Scope and Purpose of the Policy.....
9.2 Connecting Devices to the School's Systems.....
9.3 Device Monitoring.....
9.4 Security Requirements.....
9.5 Costs.....
9.6 Disciplinary Action.....
10. Staff using work devices outside school.....
10. How the school will respond to issues of misuse
11. Artificial Intelligence and Generative AI.....
12. Radicalisation and Prevent.....
13. Online safety and the 4C's
14. Monitoring arrangements.....
15. Links with other policies.....
Appendix 1: acceptable use agreement (pupils and parents/carers).....
Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors).....
Appendix 3: online safety training needs – self-audit for staff.....
Appendix 4: online safety incident report log.....
Appendix 5: Data Privacy Impact Assessment.....

1. Aims

Our school aims 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

2. Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation.

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.

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, the Online Safety Act 2023 and Teaching Online Safety in Schools (DfE 2019 (updated 2023)).

3. Roles and responsibilities

3.1 The Governing Body

The Governing Body has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

The Governing Body 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 Mrs Jillian Sutton.

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)

3.2 The Headteacher

The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The Designated Safeguarding Lead

Details of the school's Designated Safeguarding Lead (DSL) are set out in our Child Protection and Safeguarding policy.

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

- Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Headteacher, Online Safety Lead and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see appendix 4) 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 Positive Behaviour policy
- Updating and delivering staff training on online safety (appendix 3 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Headteacher and/or Full Governing Board

This list is not intended to be exhaustive.

3.4 The ICT Technician

The ICT Technician is responsible for:

- Putting in place appropriate filtering and monitoring systems, 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 on a monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Updating the school's internet search log each week and liaising with the DSL/HT when alerts are received. Safeguarding filtering categories are Abuse, Adult Content, Bullying, Criminal Activity, Radicalisation, Substance Abuse and Suicide (This list is not intended to be exhaustive.)
- The ICT technician supports the SLT to investigate the nature of the alert and the user, location in school and the content that was searched for, or had links to
- Ensuring that filtering is appropriate for primary aged pupils.
- The school uses Fortinet as its filtering and monitoring system and works with the LA to keep this up to date.

3.4.1 The Online Safety Lead

- Ensuring that any online safety incidents are logged on CPOMs and noted in the Online Incidents Log (Appendix 4) located in the Bursars office 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 Management and Positive Handling policy

3.5 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
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)
- Working with the DSL and ICT Subject Lead to ensure that any online safety incidents are logged (see appendix 4) 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.

3.6 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 as appropriate, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1)

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.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf
- How to turn on parental controls on various devices including games consoles, secure search engines, and social media apps with step by step guides: https://www.internetmatters.org/parental-controls/

3.7 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).

4. Educating pupils about online safety

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

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

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

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the Headteacher.

6. Cyber-bullying

6.1 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.

6.2 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. Teachers will discuss cyber-bullying with their classes, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health education (PSHE), activities for Safer Internet, Relationship and Sex Education part of the curriculum and other subjects were 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 (see section 11 for more detail).

The school also sends information/leaflets 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.

6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate/criminal material is suspected to be on a device, this must not be viewed. The staff member must inform the DSL or other member of the senior leadership team to decide the next course of action:

- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7. 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 and 2). Visitors will be expected to read and agree to the school's terms on acceptable use 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. Each time an employee logs into the school system they agree to abide by the terms and conditions of use.

Children are to use the computers or Chromebooks/tablets for any internet research as these devices have a higher level of filtering as set by the ICT technician. The use of Ipads for research is for the use of teaching staff only.

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

More information is set out in the acceptable use agreements in appendices 1 and 2.

8. Pupils using mobile devices in school

The school has a specific Mobile Phone policy for pupils. Pupils may bring mobile devices into school, but are not permitted to use them during:

- Lessons
- Transition between lessons
- Lunch or break times
- Clubs before or after school, or any other activities organised by the school

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendix 1).

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

Pupils' mobile phones are handed in to the class teacher at the start of the school day. These are stored securely throughout the day and pupils collect their phones (from the class teacher) when dismissed at the end of the day.

Pupils should not wear smart watches/smart glasses which have the capacity to take photographs, or send/receive messages.

9. Bring Your Own Device Policy

The School recognises that many employees will have their own personal mobile devices (such as smartphones and tablets) which they could use for School purposes and also that there can be benefits for both the School and staff in permitting such use.

However, the use of personal mobile devices for school purposes can give rise to an increased risk in terms of the security of the School's IT networks and communications systems, the protection of confidential or otherwise sensitive information and compliance with legal obligations, such as data protection requirements.

With the prior permission of their manager, employees may use a personal mobile device for school purposes, provided always that they adhere to the terms of this policy. However, employees are not required to use their personal mobile device for school purposes if they do not wish to do so.

No photographs/video of children are to be made using the employee's own device.

Before using a device under this policy for the first time, employees must erase all information and software related to any previous employment.

Staff use of their own mobile phone should only occur during non-teaching time when children are not present (such as breaktime, lunchtime and after school). Staff mobile phones should not be used during teaching sessions.

Staff need to be mindful of their responsible use of personal devices and adhere to the Teachers' Standards. Parents should not be contacted through messaging apps and personal email accounts. All email correspondence with parents should go through the Office email system.

9.1 Scope and Purpose of the Policy

This policy applies to all employees who use a personal mobile device for school purposes. It applies to use of the device both during and outside your normal working hours and whether or not your use of the device takes place at your/the School. This policy applies to all devices which are used to access the School's IT resources and communications systems, which may include smartphones, mobile phones, tablets, laptops etc.

When you access the School's systems, you may be able to access data about the School and our pupils, parents, contractors or suppliers, including information which is confidential or otherwise sensitive. When you access the School's systems using a device, the School is also exposed to a number of risks, including from the loss or theft of the device (which could result in unauthorised access to the School's systems or data), the threat of malware (such as viruses, spyware or other threats that could be introduced via a device) and the loss, wrongful disclosure or unauthorised alteration or deletion of School data (which could expose the School to the risk of non-compliance with legal obligations relating to confidentiality, data protection and privacy).

The purpose of this policy is to protect the School's systems and data and to prevent School data from being deliberately or accidentally lost, disclosed, deleted or altered, while enabling employees to access the School's systems using a device.

9.2 Connecting Devices to the School's Systems

Connectivity of all devices is managed by the IT technician, who must approve each device as providing an appropriate level of security before it can be connected to the School's systems or network. The IT technician has the absolute discretion to approve or reject a device and the School reserves the right to refuse or revoke permission for a particular device to connect with its systems, for example where a device is being or may be used in a way that puts, or could put, the School and its employees, pupils, parents, systems or data at risk or that may otherwise breach this policy. In order to access the School's systems, it may be necessary for the IT technician to install software applications on the device. If any such software is removed, access to the School's systems will be disabled.

The School has the absolute right to determine what types of data can be processed on a device and what may not and you will be advised of any types of data that is restricted or prohibited.

Where a device which is connected to the School's systems develops a technical problem, fault or failure, the IT technician will provide initial technical support to assist in determining if the issue with the device is software or hardware related. If the issue is hardware related or relates to software which you have installed, then you will be responsible for resolving it, including any repairs, maintenance or replacements costs and services. If it relates to software the School has provided, then it will provide any necessary support.

9.3 Device Monitoring

The content of the School's systems and data is the property of the School. All data, information and communications, including but not limited to e-mail, telephone conversations and voicemail recordings, instant messages and Internet and social media postings and activities, created on, transmitted to, received from, or stored or recorded on a device during the course of the School's business or on the School's behalf is the School's property, regardless of who owns the device.

The School reserves the right (remotely or otherwise) to inspect, monitor, intercept, review, disclose, remove or destroy all content on the device that has been created for or on behalf of the School and to access applications used on it for this purpose. This includes the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving, printing, removal, destruction or deletion of transactions, messages, communications, posts, log-ins, recordings and other uses of the device. It is possible that personal data may be inadvertently monitored, intercepted, reviewed or erased. Therefore, employees should have no expectation of privacy in any personal data on the device.

Employees are advised not to use the School's systems for communications of a sensitive or confidential nature because it is not guaranteed to be private.

The purposes for such monitoring are:

- to promote productivity and efficiency
- to ensure the security of the School's systems and their effective operation
- to prevent misuse of the device and protect School data
- to ensure there is no unauthorised use of the School's time or systems
- to ensure that all employees are treated with respect and dignity at work, by discovering and eliminating any material that is capable of amounting to unlawful harassment
- to ensure that employees do not used the School's facilities or systems for any unlawful purpose or activities that may damage the School's reputation
- to ensure there is no breach of confidentiality or data protection.

The School may also store copies of any content for a period of time after it is created and may delete such copies from time to time without notice.

By agreeing to use your personal mobile device for School purposes, you confirm your agreement to such inspection or monitoring and to the School's right to copy, erase or remotely wipe the entire device, including any personal data stored on the device. Although the School does not intend to wipe personal data, it may not be possible to distinguish all such information from School data. You should therefore regularly backup any personal data contained on the device.

You also agree that you use the device at your own risk and that the School will not be responsible for any loss, damage or liability arising out of its use, including any loss, corruption or misuse of any content or loss of access to or misuse of the device, its software or its functionality.

You must co-operate with the School to enable such inspection or monitoring, including providing any passwords or pin numbers necessary to access the device or relevant applications.

The School shall use reasonable endeavours not to access, copy or use any personal data held on the device, unless absolutely necessary. If such copying occurs inadvertently, the School will delete such personal data as soon as it comes to its attention.

9.4 Security Requirements

You must:

- at all times, use your best efforts to physically secure the device against loss, theft or use by persons who have not been authorised to use the device. You must secure the device whether or not it is in use and whether or not it is your current possession. This includes passwords, encryption technologies and physical control of the device
- install any anti-virus or anti-malware software at the School's request before connecting to its systems and consent to the School's procedures to manage the device and secure its data, including providing the School with any necessary passwords
- protect the device with a pin number or strong password, and keep that pin number or password secure at all times. If the confidentiality of a pin number or password is compromised, you must change it immediately
- ensure that access to the device is denied if an incorrect pin number or password is input too many times and ensure that the device automatically locks if inactive for a period of time
- maintain the device's original operating and security system and settings, and keep it current with security patches and updates
- prohibit use of the device by anyone not authorised by the School, including family and friends
- not download and install untrusted or unverified software or applications unless explicitly authorised by the School - if in doubt, contact the IT technician
- not download or transfer any restricted or prohibited types of School data to the device, for example via e-mail attachments, or store any such restricted or prohibited types of School data on the device unless you have been specifically authorised to do so, and you must immediately erase any such information that is inadvertently downloaded to the device
- not backup the device locally or to cloud-based storage applications where that might result in the backup or storage of School data and any such backups inadvertently created must be deleted immediately
- where you are permitted to store School data on the device, ensure that it is encrypted using appropriate encryption technologies approved by the IT technician.

If the School discovers or reasonably suspects that there has been a breach of this policy, including any of the security requirements listed above, it shall immediately remove access to its systems and, where appropriate, remove any School data from the device.

In the event of a lost or stolen device, or where you believe that a device may have been accessed by an unauthorised person or otherwise compromised, you must report the incident to the Headteacher and DPO immediately. Appropriate steps will be taken to ensure that School data on or accessible from the device is secured, including remote wiping of the device where appropriate. The remote wipe will destroy all School data on the device (including information contained in a work e-mail account, even if such e-mails are personal in nature). Although the School does not intend to wipe personal data, it may not be possible to distinguish all such information from School data.

On termination of employment, on or before your last day of employment by the School, all School data (including work e-mails), and any software applications provided by the School, will be removed from the device. If this cannot be achieved remotely, the device must be submitted to the IT technician for wiping and software removal. You must provide all necessary co-operation and assistance to the IT technician in

relation to this process. The same process will apply if you intend to sell the device or to return it to the manufacturer or take it to a third party for repair or replacement.

9.5 Costs

You must pay for your own device costs under this policy, including but not limited to voice and data usage charges and any purchase, repair or replacement costs. You acknowledge that you are responsible for all costs associated with the device and that your School usage of the device may increase your voice and data usage charges.

9.6 Disciplinary Action

Failure to comply with any of the requirements of this policy is a disciplinary offence and may result in disciplinary action being taken under the School's disciplinary procedure. Breach of this policy may also lead to the School revoking your access to its systems, whether through a device or otherwise.

10. Staff using work devices outside school

Employees are required to co-operate with any investigation into suspected breach, which may involve providing the School with access to the device and any relevant passwords and login details.

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 must ensure that their work device is secure and password-protected, and that they do not share their password with others. 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. Work devices must be used solely for work activities.

11. Artificial Intelligence and Generative AI

Generative AI is one type of AI. It refers to technology that can be used to create new content based on large volumes of data that models have been trained on a variety of sources.

ChatGPT, Microsoft Copilot and Google Gemini are generative AI tools, built on large language models (LLMs). LLMs are a category of foundation models trained on large amounts of data, enabling them to understand and generate human-like content.

Tools such as ChatGPT, Microsoft Copilot and Google Gemini can:

- answer questions
- complete written tasks
- generate images, text or code
- respond to prompts in a human-like way

Other forms of generative AI can produce:

- audio
- simulations
- videos

Any use of generative AI by staff, students, and pupils should be carefully considered and assessed, evaluating the benefits and risks of use.

The intended use should be specified and have clear benefits that outweigh the risks. Different considerations will apply depending on whether it is staff or pupils (especially those under 18) using AI tools.

Safety should not be compromised. Risk assessments should include plans for mitigating against unauthorised use cases.

Any use of AI and Generative AI needs to be used in consultation with the guidance in KCSiE 2026.

12. Radicalisation and Prevent

The Prevent duty is a key part of the UK government's counter-terrorism strategy. Schools are required to safeguard people from being drawn into terrorism and radicalisation. Within this online policy, the Prevent duty translates into specific technical, educational, and procedural safeguards.

- The school's Filtering and Monitoring tools will:
  - block access to extremist and terrorist content online.
  - prevent users from viewing or downloading harmful propaganda
  - detect concerning search terms, chat patterns, or attempts to bypass network blocks.

Staff must ensure that pupils are monitored whilst making online searches as part of their curriculum. Any potential breaches need to be reported in accordance with the school's safeguarding policy.Parents will be informed where necessary.

13. Online Safety and the 4C's

Staff must give consideration to the 4C's whilst teaching online safety, as well as being a user of online platforms themselves.

The 4C's are:

* Content
* Contact
* Conduct
* Commerce

The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:

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

contact: being subjected to harmful online interaction with other users or generative AI applications that simulate this; 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, including those generated using AI and online bullying

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

Where these areas are a cause of concern, they should be reported to a DSL. This will then be followed up using the school's safeguarding policy and process.

Online Sexual harassment and abuse

Through the teaching of online safety, children will need to be taught (in an age appropriate manner) the risks of:

Unsolicited sexual content online refers to any sexual content shared online which is not wanted by the recipient. This could include but is not limited to images, videos and messages seen on apps, messaging services and websites.

Image-based sexual abuse refers to the non-consensual creation and/or distribution of sexual images. This could include but is not limited to images of a sexual nature shared without the consent of the person in the photo.

Sexual coercion, threats and intimidation online could include a person receiving threats of a sexual nature or being coerced to engage in sexual behaviours on or offline via digital technologies. It could also include homophobia or transphobia online, including 'outing' or threatening to out someone. This means disclosing a person's sexuality or gender without their consent.

If a pupil, or parent, reports a concern related to the above, this should be shared with the DSL team. The procedures outlined in the school's safeguarding policy will be followed.

Online grooming in Keeping Children Safe in Education 2026 (KCSIE) is explicitly defined as a form of child sexual exploitation and abuse (CSE/CSA) that can happen directly or via digital and generative AI tools.

Key Aspects of Online Grooming in KCSIE 2026

- Grooming involves preparing a child for abuse—including via the internet—by building trust, coercion, or manipulation. KCSIE 2026 emphasizes that online grooming is part of wider child sexual exploitation and can occur over time or via a one-off digital interaction.
- **Adults Posing as Children or Peers:** The risks where adults pose as children or young adults online with the intention to groom or exploit children for sexual, criminal, financial, or other purposes.
- **Emerging Technology & AI Risks:** KCSIE 2026 expands focus on technology-enabled abuse, including AI chatbots, self-generated and AI-generated deepfake intimate images, and manipulated digital content that can facilitate or accompany grooming behaviours.

If a child makes a disclosure, this must be reported to a DSL, who will then follow the school's safeguarding policy.

14. 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 the behaviour policy. 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.

15. 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, e-bulletins and staff meetings). Staff also have specific, annual, Online Safety training delivered by trained T4T trainers in school. These trainers include the Online Safety Lead and a DSL.

The DSL 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 Whole Governing Body safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

Training records are held by the DSL and Office Manager and this record forms part of the termly safeguarding report to Governors.

More information about safeguarding training is set out in our Child Protection and Safeguarding policy.

16. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 4.

This policy will be reviewed Annually by the Online Safeguarding Lead. At every review, the policy will be shared with the Full Governing Body.

17. Links with other policies

This online safety policy is linked to our:

- Child Protection and Safeguarding policy
- Behaviour Management and Positive Handling policy
- Staff disciplinary procedures
- GDPR and Data Protection Policy and privacy notices
- Complaints procedure
- CCTV, Photography and Digital Recording policy
- Acceptable Use Policy
- Staff Code of Conduct
- Remote Learning Policy?

Version 3

Appendix 1: Acceptable Use Agreement (parents/carers to discuss with pupil as appropriate)

Acceptable use of the school's ICT systems and internet: agreement for pupils and parents/carers	
Name of pupil:	
When using the school's ICT systems and accessing the internet in school, I will not: • Use them for a non-educational purpose • Use them without a teacher being present, or without a teacher's permission • Access any inappropriate websites • Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity) • Use chat rooms • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use any inappropriate language when communicating online, including in emails • Share my password with others or log in to the school's network using someone else's details • Give my personal information (including my name, address or telephone number) to anyone without the permission of my teacher or parent/carer • Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision If I bring a personal mobile phone or other personal electronic device into school: • I will not use it during school time, clubs or other activities organised by the school, without a teacher's permission • I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online I agree that the school will monitor the websites I visit. I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others. I will always use the school's ICT systems and internet responsibly.	
Signed (pupil where appropriate):	**Date:**
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 pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 2: Acceptable Use Agreement (staff, governors, volunteers and visitors)

Acceptable use of the school's ICT systems and the 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, I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature • 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 • Share my password with others or log in to the school's network using someone else's details	
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. 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) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, 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: Online Safety training needs – self-audit for staff

Online safety training needs audit	
Name of staff member/volunteer:	**Date:**
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 pupils and parents?	
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? Please record them here.	

Appendix 4: Online Safety Incident Report Log

Online safety incident report log				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**

Appendix 5: Data Privacy Impact Assessment

Under the GDPR DPIAs should be carried for all new projects such as implementation of the new processes or systems where any of the answers to the questions on the next page are a yes.

All areas where the processing is identified as high risk should have a Data Privacy Impact Assessment and you therefore may complete this as part of your preparations for compliance with the new regulation.

Processing that is likely to result in a high risk includes (but is not limited to):

- Systematic and extensive processing activities, including profiling and where decisions have legal effects, or similarly significant effects, on individuals
- Large-scale processing of special categories of data or personal data relating to criminal convictions or offences
- Large-scale, systematic monitoring of public areas (such as CCTV)

For example, you might do this where you've considered implementing a new web monitoring system in the classroom or sharing data with a local troubled family's initiative.

A DPIA should be reviewed regularly and remain a live document and, if a data breach has occurred in an area identified as "high risk", the original DPIA should be reviewed and updated.

Where it isn't clear whether a DPIA is required, we recommend completing one, as it is a useful tool to help comply with data protection law.

A DPIA should be carried out prior to the data processing and the data controller:

- Is responsible for ensuring that the DPIA is carried out, although someone else inside or outside the school can do it
- Must seek the advice of the data protection officer. This advice, and the decisions taken by the controller, should be documented within the DPIA
- Must seek the views of data subjects or their representatives, where appropriate

While there is no legal requirement to publish a DPIA, the controller can choose to do so.

Question	Yes/No
Will individuals provide information about themselves? Will this be stored electronically? Will this be stored manually?	
What is the reason for holding this data?	
Will you make decisions or take actions form this data? Consider and detail some of the impacts should this data be incorrect, lost or stolen.	
Will the project involve the collection of new information that you have not previously held?	
Will the information be shared or disclosed to individuals who do not currently have access to this? **Note: An example of this is where you buy in a service such as milk for the children and you share details with the provider.**	
Are you implementing new technology which might be perceived as being privacy intrusive? Biometrics or facial recognition? **Note: An example of this is the implementation of a finger print payment system. The implementation of CCTV in school would be another.**	
Does the information being collected contain. Health Records, Criminal Records for example or any other information which is considered private?	
Will you to contact individuals in ways which they may find intrusive?	

The Need for the DPIA

1. *Explain why you are collecting the data.*
2. *Link any project documents. (If you are implementing a new system, the specification etc.)*
3. *Explain why you think this is "high risk".*

Data Flows

Stakeholders

Who are we consulting with to identify privacy risks?

E.g. highly sensitive data posted to the wrong location as address details not up to date.

How will it be kept up to date / reviewed?

How will it be destroyed?

Identify the Privacy and Related Risks (What are the potential problems?)

Privacy Issue	Risk to Individuals	Risk Level
E.g. highly sensitive data posted to the wrong location as address details not up to date.	*E.g. medical records included in the data which could impact the way the individual is treated by others.*	

Identify the Privacy Solutions (What can we do about it?)

Risk	Solution(s)	**Result** *(Is the risk reduced, eliminated, acceptable?)*	**Evaluation** *(Is the final impact after implementing, justified, compliant and proportionate to risk?) i.e. reduction of risk to acceptable level.*

Sign Off and Record the DPIA Outcomes

Risk	Approved Solution	Approved By	Review Date

Action Plan

Any actions should be added to the General Data Protection Compliance Action Plan and any significant risks should be added to the School risk register.

If produced for project, then individual actions can be added below:

Action to be taken	Date for completion of actions	Responsibility for action

WORLINGHAM CEVC PRIMARY SCHOOL

SAFEGUARDING STATEMENT TO ACCOMPANY POLICY DOCUMENTS

Throughout this policy runs our commitment to safeguarding the wellbeing of all our pupils at Worlingham CEVC Primary School. The values, beliefs and ethos of Worlingham Primary School are shared by all members of staff and the adherence to the guidance as stated in the school's Safeguarding Policy is of paramount importance.

The wellbeing and safety of pupils has a positive impact on their attendance, behaviour, their own Health and Safety, learning within the school environment as well as on educational visits.

Throughout the curriculum children are taught how to manage risk and how to keep themselves safe. The children know that if they need help they can talk to a member of staff at school. Children are taught how to keep themselves safe whilst using ICT equipment and are instructed to report any inappropriate material to the member of staff leading the session.

Children who have an identified SEN which creates difficulties with communication may need additional support in expressing concerns to a member of staff. Staff will need to follow the guidance in the safeguarding policy when dealing with a disclosure, taking into account the ability of the individual.

A copy of the Safeguarding policy can be found on the school website, in the Headteacher's office and also the staff room. This policy provides comprehensive detail in identifying types of abuse and the procedures that need to be followed.

Within the Safeguarding Policy is a section on The Prevent Duty and what it means for our School.