Ashford CE Primary School

Computing and Online Safety Policy

Updated Policy: June 2026 Signed: L Bowman

Approved by FGB: 11 June 2026 Chair of Governors

Next Review: September 2026 for updates and changes to Keeping Children Safe in Education

Computing and Online Safety Policy

Our School Vision

We are a caring Christian community where everyone adopts an "I can" attitude; everyone feels valued, safe and loved by God. We celebrate our God-given individuality, achievements and talents and we aspire, with God's help, to become the best that we can be. We believe that each one of us has the ability to achieve our highest potential, living and learning in the fullness of God.

I can do all things through Christ who gives me strength.

Philippians 4v13

Aims Of This Policy:

At Ashford CE Primary school our aim is to inspire, engage and encourage our pupils to have high aspirations for themselves, doing everything using their growth mindset and an 'I can' attitude. It is also our job to ensure that our children feel safe and happy in the world they both live and learn in. It is with this aim, that our Computing curriculum works hand-in-hand with our safeguarding procedures to ensure that our children are safe and content in the digital world.

As a school it is our mission to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- 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 (which we refer to as 'mobile phones')
- Establish clear expectations for the way all members of the school community engage with each other online and establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk. These being the 4 C's:

- Content – being exposed to illegal, inappropriate or harmful content, such as pornography, misinformation, disinformation (including fake news), conspiracy theories, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- Contact – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit the user for sexual, criminal, financial or other purposes
- Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as 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

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', as well as 'Preventing and tackling bullying and cyber-bullying: advice for Headteachers and school staff'. It also refers to the DfE's guidance on protecting children from radicalisation.

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
- Meeting digital and technology standards
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- [Relationships and sex education (RSE) and health education
- 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 Body

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

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

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

The governing board will make sure that the school teaches pupils how to keep themselves and others safe, including online.

The governing board will make sure that the school has appropriate filtering and monitoring systems in place on school devices and school networks and will regularly review their effectiveness. The board will review the DfE's filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems
- Reviewing filtering and monitoring provisions at least annually
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning
- Having effective monitoring strategies in place that meet the school's safeguarding needs

The Governing Board has appointed a governor to oversee online safety in the school.

All governors will:

- Make sure 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)
- Make sure that online safety is a running and interrelated theme when devising and implementing the whole-school or college approach to safeguarding and related policies and/or procedures
- Make sure 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

The Headteacher

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

The Designated Safeguarding Lead

Details of the school's designated safeguarding lead (DSL) and deputies are set out in our Safeguarding Children Policy, School Handbook and on posters displayed around the school and on the website. It is also included in relevant job descriptions. The DSL is currently the Headteacher.

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

- Supporting the Senior Leadership Team (SLT) in making sure that staff understand this policy and that it is being implemented consistently throughout the school

- Working with the SLT and governing board to review this policy annually and make sure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the Headteacher, ICT 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's child protection policy
- Responding to safeguarding concerns identified by filtering and monitoring/SENSO
- Making sure that any online safety incidents are logged within CPOMS (see appendix 3) and dealt with appropriately in line with this policy
- Making sure that any incidents of cyber-bullying are logged within CPOMS and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 4 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 governing board
- Undertaking annual risk assessments that consider and reflect the risks pupils face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

The IT Consultant in conjunction with the Computing Lead and SBM is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and make sure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Making sure 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 monthly
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Making sure that any online safety incidents are logged in CPOMS and dealt with appropriately in line with this policy
- Making sure 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.

- Computing Lead will liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated.
- Computing Lead will work with the DSL to develop a planned and coordinated online safety education programme. This will be provided through:
    - The computing curriculum
    - PHSE and SRE programmes (Jigsaw)
    - A mapped cross-curricular programme
    - Worship and pastoral programmes through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

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 making sure that pupils follow the school's terms on acceptable use (appendix 1)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by adding an incident to CPOMS if related to a pupil or by contacting the SBM and IT Consultant

› Following the correct procedures contacting the IT Consultant if they need to bypass the filtering and monitoring systems for educational purposes

- Working with the DSL to make sure that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
- Making sure 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 sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'
- Modelling safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media in line with the staff Code of Conduct.

This list is not intended to be exhaustive.

Parents and Carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the online services and devices in an appropriate way. According to 2023 Ofcom research, 93% of children aged 5 - 7 years watch videos on video-sharing platforms (VSPs) like YouTube and TikTok. Parents are encouraged to be aware of their child's screen time, online safety and activity outside of school. Parents should be aware that some online activities have age restrictions because they include content which is not appropriate for children under a specific age. However, research shows that 30% of 6–10 year olds are accessing messaging apps with an age restriction of 16 years.

Parents/carers are expected to:

- Notify a member of staff or the Headteacher of any concerns or queries regarding this policy
- Make sure that their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

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

- What are the issues? – UK Safer Internet Centre
- Help and advice for parents/carers – Childnet
- Parents and carers resource sheet – Childnet
- Try to attend school workshops that are run in line with Safer Internet Day.

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 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

Pupils will be taught about online safety as part of a rich Computing curriculum. The text below is taken from the National Curriculum computing programmes of study and the government's guidance on relationships education, relationships and sex education (RSE) and health education (for introduction 1 September 2026).

All schools have to teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

In **Key Stage (KS) 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 (KS) 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
- Be discerning in evaluating digital content

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

- That people should be respectful in online interactions, and that the same principles apply to online relationships as to face-to-face relationships, including where people are anonymous. For example, the importance of avoiding putting pressure on others to share information and images online, and strategies for resisting peer pressure
- How to critically evaluate their online relationships and sources of information, including awareness of the risks associated with people they have never met. For example, that people sometimes behave differently online, including pretending to be someone else, or pretending to be a child, and that this can lead to dangerous situations. How to recognise harmful content or harmful contact, and how to report this
- That there is a minimum age for joining social media sites (currently 13), which protects children from inappropriate content or unsafe contact with older social media users, who may be strangers, including other children and adults
- The importance of exercising caution about sharing any information about themselves online. Understanding the importance of privacy and location settings to protect information online
- Online risks, including that any material provided online might be circulated, and that once a picture or words has been circulated there is no way of deleting it everywhere and no control over where it ends up
- That the internet contains a lot of content that can be inappropriate and upsetting for children, and where to go for advice and support when they feel worried or concerned about something they have seen or engaged with online

At Ashford CE we celebrate Safer Internet Day and regularly promote key guides to keeping ourselves and each other safe. Information is shared with parents on our school Facebook page, as well as regular updates in our school newsletter.

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.

Pupils will be taught practical cyber security skills

The following items come from the DfE's non-statutory cyber security standards for schools and colleges.

All pupils will receive age-appropriate training on safe internet use, including:

- Methods that hackers use to trick people into disclosing personal information
- Password security
- Social engineering
- The risks of removable storage devices (e.g. USBs)
- Multi-factor authentication
- How to report a cyber incident or attack
- How to report a personal data breach

Pupils will also receive age-appropriate education on safeguarding issues such as cyberbullying and the risks of online radicalisation.

Educating Parents/Carers About Online Safety

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

Online safety will also be covered during parents' evenings.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access

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

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

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 encourage them 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. Class teachers will discuss cyber-bullying with their classes.

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 sends information/leaflets on cyber-bullying to parents/carers so 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's Positive Behaviour Management 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.

Examining Electronic Devices

The Headteacher, and any member of staff authorised to do so by the Headteacher, can carry out a search of belongings and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the Headteacher
- Explain to the pupil why their belongings are being searched, and how the search will happen; and give them the opportunity to ask questions about it
- Seek the pupil's co-operation
- If the member of staff has assessed that the device maybe on the child rather than in their belongings, they will seek the pupil's co-operation to hand over the device. If they refuse the parent will be asked to come to school to see whether the pupil has a hidden device on their person.

Authorised staff members may examine and, in exceptional circumstances, erase any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the Headteacher to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding whether there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils belongings will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

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

It is school policy that only those pupils who have permission to walk home alone can bring a device such as a phone to school. Pupils in Year 5 & 6 with this permission from their parents/carers will enter and exit through the Hall doors. Phones must be turned off before entering and handed to a member of staff for storage through the school day. Phones are only handed back when a pupil leaves school or at the end of the school day as they leave through the hall. Cases where a pupil is found to have a phone/device and have not followed school rules will be subject to a sanction as outlined in the School's Positive Behaviour Policy and Mobile Phone Policy.

Artificial Intelligence (AI)

Generative AI tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

Ashford CE Primary School recognises that AI has many uses to help pupils learn but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

Ashford CE Primary School will treat any use of AI to bully pupils very seriously, in line with our anti-bullying policy.

Staff should be aware of the risks of using AI tools while they are still being developed and should carry out a risk assessment where new AI tools are being used by the school, and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by them, including, but not limited to, pupils and staff.

Acceptable Use Of The Internet In School

All pupils, parents/carers, 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.

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

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

Staff Using Work Devices Outside School

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords can be made up of 3 random words, in combination with numbers and special characters if required, or generated by a password manager
- Ensuring their hard drive is 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 device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by promptly installing the latest updates

Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in appendix 2.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from SBM and IT Consultant

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 internet acceptable use. 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 or 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 that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Training For Staff, Governors And Volunteers

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).

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, threatening, 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

The DSL Team 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.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our Safeguarding Children Policy.

Data Security

The school is responsible for making sure it has the appropriate level of security protection and procedures in place to safeguard its systems, staff and pupils. It therefore takes steps to protect the security of its computing resources, data and user accounts. The effectiveness of these procedures is reviewed periodically to keep up with evolving cybercrime technologies.

Staff, volunteers, pupils and others who use the school's ICT facilities should use safe computing practices at all times. We aim to meet the cyber security standards recommended by the Department for Education's guidance on digital and technology standards in schools and colleges, including the use of:

- Security features
- Firewalls
- User authentication and multi-factor authentication
- Anti-malware software

Passwords

All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Members of staff or pupils who disclose account or password information may face disciplinary action.

Remote Access

Staff accessing the school's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on site. Staff must be particularly vigilant if they use the

school's ICT facilities outside the school and must take such precautions against importing viruses or compromising system security.

Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy.

Equalities Statement

Ashford Church of England Primary School is committed to valuing diversity and to equality of opportunity. We aim to create and promote an environment in which pupils, parents and staff are treated fairly and with respect, and feel able to contribute to the best of their abilities.

The Governing Body recognise that it is unlawful to consider anyone's gender, marital status, colour, race, nationality, ethnic or national origin, disability, religious reliefs, age or sexual orientation.

Full consideration has been given to this during the formulation of this policy as it is the Governors' aim that no one at Ashford Church of England Primary School should suffer discrimination, either directly or indirectly, or harassment on any of these grounds.

Monitoring Arrangements

The DSL logs behaviour and safeguarding issues related to online safety. Incidents are logged on CPOMs under the appropriate category.

This policy will be reviewed every year by the Headteacher. At every review, the policy will be shared with the governing board. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

Links with Other Policies:

This online safety policy is linked to our:

- Safeguarding Children Policy
- Positive Behaviour Management Policy
- Anti Bullying Policy
- Staff Disciplinary Procedures
- Staff Code of Conduct
- Data Protection Policy and Privacy Notices
- Acceptable Use Agreements
- Complaints Procedure

Appendix 1

Acceptable Use Agreement:

ACCEPTABLE USE OF THE SCHOOL'S COMPUITNG SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
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 my 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
• 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:**
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 will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 2

2025/26

ACCEPTABLE INTERNET & E-SAFETY USE

CONDUCT FOR STAFF, THIRD PARTY STAFF, VOLUNTEERS Including PTA TRUSTEEs AND GOVERNORS

This policy applies to all persons within the school organisation who may at any time have access to school technology or network or email.

ACCEPTABLE INTERNET & ONLINE SAFETY USE

- Private use of the internet may only take place outside of teaching/school hours (professional development activities are not deemed private). However, the school computers may not be used for the purpose of social networking unless authorised school activity/promotion.
- Receiving questionable material or chancing upon an undesirable website should be notified to the Headteacher/School Business Manager (SBM) immediately.
- Emails sent to an external organisation should be written carefully and checked before sending in the same way as a letter written on school headed paper. **Avoid the autofill of contacts facility and check recipients before sending to ensure information remains secure, including if email addresses should be entered into the cc or bcc field**. If use of autofill results in breaches of data protection this facility will be disabled.
- Encrypt or Pin protect any document containing sensitive information before sending it to any recipient. Agree the PIN code via another communication method – phone, text as appropriate.
- Keep personal details safe and do not give them out over the internet or phone.
- Everyone should develop and maintain knowledge of internet safety issues, particularly with regard to how they might affect children.
- Only the school's approved Internet Service Provider (ISP) – RM SafetyNet, should be used for school internet use.
- Change school passwords every half term to a "strong" password which includes capitals, lower case, numbers and symbols and should contain at least 8 characters.
- Ensure that the password auto-save function is turned off on shared computers.
- Ensure that you are the only one who knows and uses your user Account and understand that anything undertaken while you are logged in will be your responsibility.

Lock your computer whenever you leave it unattended. (Windows key +L)

- Report any suspicious emails, before clicking on any links, downloading any attachments or entering your user details. When you report it, do not forward the email but send a screen shot.
- Ensure that personal data is kept secure and is used appropriately, whether in the office, or when working remotely. Personal data should be stored on the school server or on the school SharePoint
- **When accessing emails on a computer linked to an interactive board, ensure that the board is switched off so that no one can accidently see any confidential emails**.

UNACCEPTABLE USE OF THE INTERNET

- It is not acceptable to access, transmit or create any offensive, obscene or indecent images, sounds, data or other material, as well as material that is defamatory, violent, abusive, racist, homophobic or transphobic material or anything that may cause needless anxiety.
- Bringing the name of the school into disrepute.
- Breach of confidentiality that results in information being inappropriately made available to others, including through social networking sites used from phones and home computers.
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of data protection legislation
- Transmission of commercial or advertising material or access to gambling websites.
- Violation of the Data Protection Act 2018 by deliberately corrupting or destroying other users' data or violating privacy of others.
- Disrupting the work of others or wasting the time of staff or other users.
- Do not upload a photo to your email profile.

This is not an exhaustive list. The school reserves the right to amend this list at any time. The Headteacher will use their professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities. Staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the school's policies.

ACCESS TO SCHOOL ICT FACILITIES AND MATERIALS

The school's SBM and ICT Provider manage access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:

- Computers, tablets and other mobile devices
- Access permissions for certain programmes or files
- Use of copier facilities

Personal use of ICT facilities including copying must not be overused or abused.

Only devices supplied by the school should be used to access the school network, as they will have the required level of security and protection. Authorised users will be provided with unique log-in/account information and passwords that they must use when accessing the school's ICT facilities. One User, One Login. Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the SBM.

FILTERING & MONITORING

The school's filtering and monitoring will be reviewed regularly, and details of blocked searches will be reported at DSL meetings and to the Full Governing Body in line with advice in KCSIE 2023.You should be aware of the filtering arrangements via RM SafetyNet and should report any sites which should have been filtered to the SBM. Staff can also ask for suitable educational sites to be "whitelisted" if they are currently blocked. There is a file for recording inappropriate sites in the PPA room. You should also notify the SBM by email.

The school's network is monitored using SENSO. This is loaded on all pupil devices. It will also be added to all computers with shared users including the hall and PPA room. SENSO recognises keystrokes as well as searches and the DSL team receive alerts for serious concerns. Please alert DSLs if your current lessons might cause an increase of false positive alerts.

Whilst filtering & monitoring provides a good level of security it does not guarantee 100% security. **Staff must remain vigilant of pupil activity on devices.**

USE OF AI

Artificial Intelligence (AI) has many uses for teaching and learning as well as realising time efficiencies, but that it also poses risk to personal data. Therefore, the school workforce

- Never share or input any personal data to a free AI platform e.g. Chat GPT, DeepSeek, Google Gemini, Grammarly.
- Ensure before they use any AI tool it is reviewed and authorised by the School and only use it for the tasks which have been authorised.
- Understand that if personal data is entered into a free AI platform or into an AI Tool for a task which has not been authorised then it will either be considered a Data Breach or breach of this ICT User Agreement and could be subject to staff disciplinary proceeding

USE OF EMAIL

- The school provides each member of staff, Governors and the PTA with an email address. This email account should be used for school purposes only. Unless with the specific agreement of the SBM or Headteacher.
- Governors should use the agreed SharePoint file for sharing documents and information in relation to their role as governors. Any information downloaded from SharePoint onto a personal device should be deleted upon the completion of the task.
- All work-related business should be conducted using the email address the school has provided. Personal email addresses or mobile number should not be used.
- Staff must not share their personal email addresses with parents and pupils and must not send any work-related materials using their personal email account.
- Users must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.
- Understand that anything written in an email or document about an identifiable person can be requested via a Subject Access Request and read by that individual. Therefore, do not write anything that you would not want that person to read, or that could bring the organisation in disrepute or is counter to the staff code of conduct. This includes the use of emojis, exclamation marks and sarcasm. Consider if the communications you send breach confidentiality or the Data Protection Act, by asking "should the recipient view this information".
- Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information, or the data of multiple individuals should be encrypted so that the information is only accessible by the intended recipient. Please ensure that pupils are only named using initials in emails.

- If Users receive an email in error, the sender should be informed, and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information. The SBM should be informed immediately so that this can be recorded in the Record of Breaches register under the section “received in error – breach by another organisation”
- If staff send an email in error which contains the personal information of another person, they must inform the SBM immediately and follow our data breach procedure.

USE OF PHONES

- Staff must not give their personal phone numbers to parents or pupils.
- School phones must not be used for personal matters.
- Staff who are provided with the use of a mobile phone as equipment for their role must abide by the same rules for ICT acceptable use.
- The school can record in-coming and out-going phone conversations.
- If you record calls, callers **must** be made aware that the conversation is being recorded and the reasons for doing so.
- Mobile phones and personally owned devices may not be used in any way during lesson time unless permission is given by the Headteacher. They should be switched off or silent at all times and stored securely out of sight of others. Staff using smart watch technology should ensure that they do not read and respond to messages during lesson time. Where phones are used outside of lesson time such as at breaktime they must **not** be used in an area where there are children present. Suitable locations may be the staffroom, PPA room, offices or outside of the school site.
- No images or videos should be taken on mobile phones or personally owned devices. It is not permitted to take photos or videos of children on personal devices. Where photos are taken at staff social events, these should not be published without the express agreement of the people involved.
- Staff are not permitted to use their own mobile phones for contacting children or their families within or outside of the school in a professional capacity unless this is during a lockdown or as a result of self-isolation. This should be agreed with SLT and ensured that the number is withheld.
- Staff should never send to, or accept from anyone, texts or images that could be viewed as inappropriate or allow children to be ‘friends’ on social networking sites.
- All users with school emails should ensure their phones are protected with PIN codes or other security in case of loss or theft. A number of websites now require two-step authentication and therefore it is accepted that staff may use their phones to be able to access approved sites.
- Staff should never store parents or pupil’s telephone numbers on their mobile phone, as this allows the possibility of inappropriate contact. Where staff have friends, who are also parents a clear distinction should be made when in contact. Any matters raised about the school should be treated with care and referred to the appropriate person within school. Staff should take particular care when asked questions as these can be reported back to the school as “Mr/Mrs X said....”
- The taking of personal phone calls during work time should be kept to a reasonable minimum and should generally relate to emergency situations.
- Staff can give the school office number as an emergency contact number for dependents during the working day to minimise the need for checking mobile phones.

- WhatsApp is/is not an approved communication channel for the school. As this is not a school-controlled platform, The school is not able to monitor or easily access the information held. This can cause issues if there were to be a Subject Access or Freedom of Information Request. Any existing WhatsApp group containing staff should not show any affiliation with the school via the name.

SOCIAL MEDIA

Staff should take care to follow the school's guidelines on social media use.

MONITORING OF SCHOOL NETWORK AND USE OF ICT FACILITIES

The school reserves the right to monitor the use of its ICT facilities and network, and access accounts when deemed necessary This includes, but is not limited to, monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications
- CCTV footage
- SENSO alerts

Only authorised ICT staff may inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

The school monitors ICT use in order to:

- Obtain information related to school business
- Investigate compliance with school policies, procedures and standards
- Ensure effective school and ICT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

MEMORY STICKS

All staff have a duty of care to ensure all confidential, sensitive and personal information is held securely at all times. The use of non-encrypted memory sticks is prohibited, and staff members found using them may be subject to disciplinary procedures. Any loss of encrypted memory sticks must be reported to the SBM. Confidential, Sensitive and Personal Information Data must not be stored or

carried on non-encrypted memory stick, laptops or computers, or emailed to personal email accounts.

All members of staff who use memory sticks will be supplied with an encrypted one. This memory stick belongs to the school. However, on leaving staff will be permitted to retain their memory stick on the understanding that they sign a written declaration that any information in any form relating to the school has been deleted. If the memory stick gets lost you must inform the Headteacher immediately and will be charged £10.00 for a replacement. If the memory stick is stolen you must contact the Headteacher immediately and provide the school with a crime number.

REMOTE ACCESS TO SCHOOL COMPUTERS, PROVIDING REMOTE EDUCATION AND VIRTUAL MEETINGS

Ashford CE Primary School and our IT services, support secure, safe, accessible and available remote access and mobile working through its systems and policies, through the provision of essential technical controls and through raising user awareness and encouraging good working practices. Users with remote access permissions must be aware of procedures and responsible ethical practices.

Remote Access - accessing the school's network from outside of the premises via a different network.

Mobile Working - performing tasks on the network, from connectivity outside of the network (i.e. the creation, storage, processing and transport or transfer of data/ information) as an employee of Ashford CE Primary School.

The primary responsibilities of employees and other users that remotely log into the school's network are to:

- Know what information they are accessing, using or transferring
- Understand and adhere to contractual, ethical or other requirements attached to the information and pertinent to school policies and procedures.
- Users are responsible for following correct procedures when logging out of the remote session
- Confidential data/information should not be created or stored on privately owned computers. The school strongly encourages the use of the Microsoft Office 365 facilities for working online and storing on the OneDrive or SharePoint facilities.

If users are using their own personal systems or other mobile devices to carry out work for Ashford CE Primary School then the following points should be noted and followed:

- Keep abreast of current security threats and issues for their device type, whether that is related to hardware or software
- Maintain safe web-surfing practice.
- Each device is equipped with up-to-date anti-virus software and other security software such as malware and a configured firewall.
- They perform critical operating System updates as soon as they become available.
- They practice good password controls as appropriate.

- They do not respond to unsolicited emails or click any link within unsolicited emails, pop-ups and other means of communication that is not relevant to their role.
- Mobile devices are not left unattended or data that is deemed confidential data is left visible on the screen in public areas.
- If the system has suffered loss of data, corruption of data or any other issues that may impact the network or other systems at Ashford CE Primary it is reported as soon as possible to the SLT and IT support at the School.

The standards and expectations listed above are all to be maintained when organising distance-learning opportunities for children or online sessions/meetings. When using Zoom, Teams or any other platform to hold meetings for or about children, the following points should be noted in addition to those above.

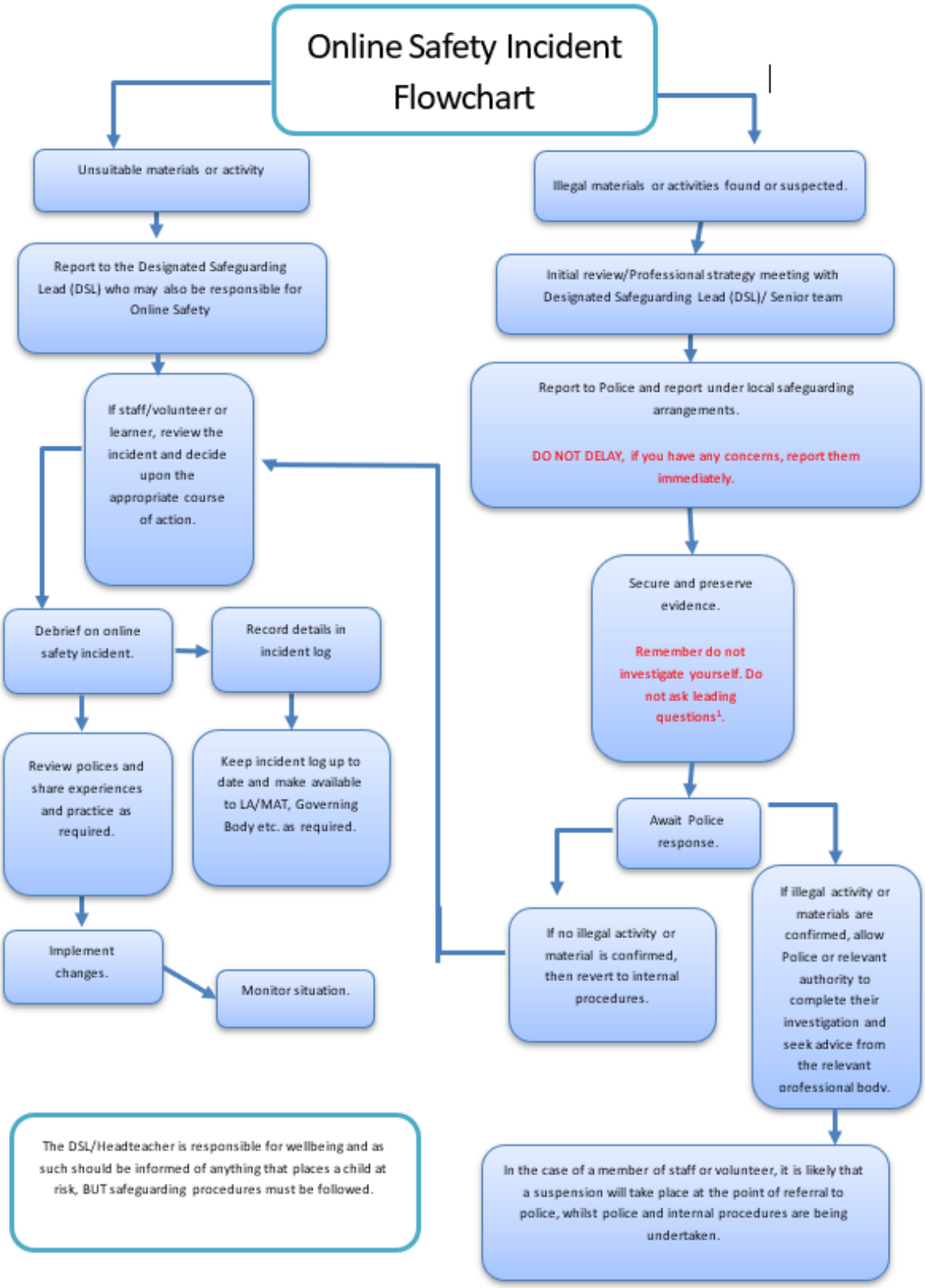
- If hosting from home, please be appropriately dressed and ensure, as far as possible, that there are no features in the background that might give clues as to your home address.
- Ensure that there are no items in the background that might be deemed inappropriate or unprofessional (piles of washing, etc.).
- All meetings should be password protected to avoid uninvited participants. Ensure all participants are named before admittance and are not admitted under unrecognised handles such as ‘Ipad7’ or ‘LizardBoy’.
- It is best practice to have two staff members present during a Zoom/online meeting where possible.

Please sign below to say that you have read and understood this information.

Name: **Signature:**

Date:

Appendix 3


Online Safety Incident Flowchart
Unsuitable materials or activity
Report to the Designated Safeguarding Lead (DSL) who may also be responsible for Online Safety
If staff/volunteer or learner, review the incident and decide upon the appropriate course of action.
Debrief on online safety incident.
Record details in incident log
Review polices and share experiences and practice as required.
Keep incident log up to date and make available to LA/MAT, Governing Body etc. as required.
Implement changes.
Monitor situation.
Illegal materials or activities found or suspected.
Initial review/Professional strategy meeting with Designated Safeguarding Lead (DSL)/ Senior team
Report to Police and report under local safeguarding arrangements.
DO NOT DELAY, if you have any concerns, report them immediately.
Secure and preserve evidence.
Remember do not investigate yourself. Do not ask leading questions[1].
Await Police response.
If no illegal activity or material is confirmed, then revert to internal procedures.
If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body.
In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.
The DSL/Headteacher is responsible for wellbeing and as such should be informed of anything that places a child at risk, BUT safeguarding procedures must be followed.

Appendix 4

Online Safety Training Needs – Self-Audit For Staff

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?	
Are you aware of the ways pupils can abuse their peers online?	
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/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
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?	