Online Safety and Acceptable Use Policy

Formally adopted by the Governing Board/ Trust of:	**Ashwicken VA Primary School**
On:-	**Summer 25**
Chair of Governors:	**Murree Groom**
Last updated:-	

Date of Last Review:	**Summer 2025**	*Next Review Date:*	**Summer 2026**	*Reviewing Body:*	**Full Governing Body**

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. Staff using work devices outside school

10. How the school will respond to issues of misuse

11. Training

12. Monitoring arrangements

13. Links with other policies

14. Appendix 1: Further information on acceptable use of email, website digital content and social media

15. Appendix 2:: Acceptable use agreement (staff and governors)

16. Appendix 3: Online safety training needs – self-audit for staff

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

The four key categories of risk

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

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as child-to-child 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** – 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

2. Legislation and guidance

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

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

3. Roles and responsibilities

31 The governing board

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

All governors will:

- Ensure that they have read and understand this policy
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND 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.

32 The headteacher

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

33 The designated safeguarding leaders

Details of the school's designated safeguarding leaders (DSLs) are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The DSLs take 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 and relevant staff to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety or cyber-bullying incidents are logged on CPOMs and dealt with appropriately in line with this policy and the behaviour policy. These incidents will be discussed in safeguarding meetings that are attended by DSLs
- Updating and delivering staff safeguarding training, that include information regarding online safety
- Liaising with other agencies and/or external services if necessary

This list is not intended to be exhaustive.

34 The ICT manager (through JC Comtech)

Working alongside the Senior Leadership Team and the service provided by Norfolk County Council, the ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a weekly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

This list is not intended to be exhaustive.

35 All staff and regular 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, and ensuring that pupils follow the school's terms on acceptable use (signed for by staff on induction and annually at September INSET)
- Ensuring that any online safety and cyber-bullying incidents are logged on CPOMs
- 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'

This list is not intended to be exhaustive.

36 Parents

Parents are expected to:

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

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

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International

37 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.

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum. The text below is taken from the National Curriculum computing programmes of study. It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education. All schools have to teach Relationships education and health education in primary schools.

In Key Stage 1, pupils will be taught to:

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

Pupils in Key Stage 2 will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the end of primary school, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

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.

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 or online learning platforms.

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 DSLs.

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

6. Cyber-bullying

61 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.

62 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.

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 through our newsletter, 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 DSLs 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.

63 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 material is found on the device, it is up to the staff member in conjunction with the DSLs or other member of the senior leadership team to decide whether they should:

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

* If a staff member believes a device may contain a nude or semi-nude image or an image that it's a criminal offence to possess, they will not view the image but will report this to the DSLs (or equivalent) immediately, who will decide what to do next. The DSLs 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.

** Staff will also confiscate the device to give to the police, if they have reasonable grounds to suspect that it contains evidence in relation to an offence.

Any searching of pupils 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.

7. Acceptable use of the internet in school

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

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

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

8. Pupils using mobile devices in school

Pupils are not allowed a mobile phone or any other device that connects to the internet in school. If they bring a mobile phone or any other device that connects to the internet into school (which a parent must agree to), they have to leave it in a secure location in the school office at all times during the school day.

9. 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 are recommended (at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters)
- 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 (this is done through our ICT partner, JCComtech
- Keeping operating systems up to date by always install the latest updates (this is done through our ICT partner, JCComtech)
- If staff are bringing their own device to work, they have to agree to and sign to say that they have agreed to a protocol (Bring your own device policy) for this on CPOMS

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 3. 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 the Senior Leadership Team.

10. 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. 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 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.

11. Training

All new staff members will receive training at least annually on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails and staff 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, 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 DSLs will undertake child protection and safeguarding training, which will include online safety. 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 child protection and safeguarding policy.

12. Monitoring arrangements

The DSLs and members of staff log behaviour and safeguarding issues related to online safety using CPOMs.

This policy will be reviewed every year by the Senior Leadership Team. 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.

13. Links with other policies

This online safety policy is linked to our:

- School safeguarding policy
- Internet, Social Media and Email Use Policy
- Cyberbullying Policy
- Anti-bullying policy
- Behaviour policy
- Complaints procedure
- Computing Curriculum

Appendix 1: Further information on acceptable use of email, website digital content and social media

E-mail

We provide staff and all children with an email account for their professional/educational use only. Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material

Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

The content of these emails should be respectful and be fairly formal in style, as appropriate to a school setting. There may be times where teachers and staff use Microsoft Teams to conduct short video calls with the class as a whole. 1:1 video meeting should only happen where this has been arranged in advance and with appropriate parent/ carer permission. Staff would almost always make these calls from a school setting, and another member of staff should be able to overhear or oversee the meeting. When staff have to make video calls from a setting other than school, they are reminded to always remain professional during these meetings and therefore thinking carefully about the background of their video call etc.

The official school email service is regarded as safe and secure and is monitored and is the only email address which should be used to contact parents.

Any digital communication between staff and pupils or parents / carers (email, social media, etc.) must be professional in tone and content.

School website

The school website complies with statutory DfE requirements. Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status. Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with GDPR with regards the use of such images. Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs Permission from parents or carers will be obtained before photographs of pupils are published on the school website or on other platforms.

Digital Content

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet.

Digital images and video

We gain parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter/son joins the school.

We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs.

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.

Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute. Pupils and

parents/ carers must not take, use, share, publish or distribute images of others without their permission, *although parents and others attending organisation events are allowed to take photographs and videos of those events for domestic purposes, unless specifically asked not to. (Please see our Data Protection Policy for further information).*

Staff mobile phone communication should be used sparingly and only when necessary; children should not be present unless necessary. All staff are encouraged to leave mobile phones switched off in their bags which should be left in a classroom cupboard or other safe place during lesson times. If staff expect to receive a call during lesson time they should direct the caller to the school landline in the office. If/when the call is made the member of staff will be informed by the office and if necessary, given time to leave the classroom to return or take the call.
The school permits the use of personal mobile phones on trips to contact the school if/when appropriate and necessary. The school does have its own mobile phone and this should be used in all out of school circumstances where possible. The use of mobile phones to record images from the visit is not permitted.

Social Media
Ashwicken VA Primary School understands that social media is a growing part of life outside of school. We have a responsibility to safeguard our pupils against potential dangers when accessing the internet at school, and to educate our pupils about how to protect themselves online when outside of school. This school defines social media as any online platform that offers real-time interaction between the user and other individuals or groups including:
•Blogs
•Online discussion forums
•Collaborative spaces such as Facebook
•Media sharing services such as YouTube
•Micro-blogging applications such as Twitter
We would define 'member of the school community' as any teacher, member of support staff, pupil, parent/carer of a pupil, governor and member of the school kitchen staff.

Social media use –staff

•School social media passwords are kept in the office.
•The head teacher is responsible for the school's social media accounts
•Staff must not access social media during lesson times unless it is related to the learning activity
•Staff may use social media during their break times but not in front of pupils.
•Members of staff must not 'friend' or otherwise contact pupils or parents through social media.
•If pupils or parents attempt to 'friend' members of staff through social media they should ignore requests.
•Members of staff should avoid identifying themselves as an employee of the school on social media.
•Members of staff must consider carefully the content of anything they post online and refrain from anything which is damaging to the school or any of its staff or pupils
•Where teachers or members of staff use social media in a personal capacity, they should make it clear that their views are personal. Staff may 'like' and 're-tweet' but not tweet about the school from their personal account.
•Staff who also have links with parents should consider very carefully their use of any social media with due regard to those they are friends with, what they post. They should never make comments about the school or any staff or pupils. This will link to all the other points in this section.
•Teachers or members of staff must not post any information which could identify a pupil, class or the school.

•Members of staff should not post anonymously or under an alias to evade the guidance given in this policy. •Breaches of this policy by members of staff will be taken seriously, and in the event of illegal, defamatory or discriminatory content, could lead to prosecution, disciplinary action or dismissal. •Members of staff should be aware that if their out-of-work activity brings the school into disrepute, disciplinary action will be taken. •Members of staff should regularly check their online presence for negative content via search engines. •If inappropriate content is accessed online, an inappropriate website content report form should be completed and passed on to the Headteacher. •Attempts to bully, coerce or manipulate members of the school community, via social media, by teachers and members of staff will be dealt with as a disciplinary matter. •Staff members should use their school email address for school business and personal email address for their private correspondence; the two should not be mixed.
Social media use –pupils and parents/carers •Pupils should not access social media during lesson time as the school does not advocate the use of social media sites for children in the primary age range. •Breaches of this policy by pupils will be taken seriously, and in the event of illegal, defamatory or discriminatory content could lead to prosecution, or exclusion. •Pupils and parents/carers are requested not to attempt to "friend" or otherwise contact members of staff through social media. If attempts to contact members of staff through social media are made, they will be reported to the Headteacher. •If members of staff attempt to "friend" or otherwise contact pupils or parents/carers through social media, they should be reported to the Headteacher. •Pupils and parents/carers should not post anonymously or under an alias to evade the guidance given in this policy. •Pupils and parents/carers must not post content online which is damaging to the school or any of its staff or pupils. •Pupils at Ashwicken VA Primary School should not sign up to social media sites that have an age restriction above the pupil's age and parents/ carers should monitor this. •If inappropriate content is accessed online on school premises, it must be reported to a teacher

Appendix 2: Acceptable use agreement

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS WHO ARE LEFT UNACCOMPANIED.
Name of staff member/governor/volunteer/visitors:
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Take photographs of pupils unless for an educational purpose and only on a school mobile or ipad • Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) know if a pupil informs me they have found any material which might upset, distress or harm them or others, 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**:
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 home school 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?	