St Andrew's CE VC Primary School

'Roots to grow, Wings to fly'
They will soar on wings like Eagles.

Isaiah 40:31

Online Safety Policy

Signed (Chair)	Name Anthony Parker	Date 12th February 2026
Signed (Head)	Name Graham Pike	Date 12th February 2026
Ratified by Governing Body on		Next Review February 2027

Equality Impact Assessment (EqIA)

This policy has been assessed with regard to its impact on equalities issues. The equality impact assessment has been conducted by the relevant Governors' sub-committee and focused on race, gender, disability, age, sexual orientation, gender identity and religion/belief. Community Cohesion has also formed part of the impact assessment work in order to ensure respect for diversity, alongside a commitment to common and shared bonds.

EqIA outcomes

[X] *The assessment found no areas of potential negative impact and actions resulting in positive impact are in place.*

Online Safety Policy

Contents

1 Aims

Our school aims 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 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:

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 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 – 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;
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 considers the National Curriculum computing programmes of study.

3 Roles and responsibilities:

3.1 The governing board:

The governing board has overall responsibility for monitoring this policy and holding the Head Teacher 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, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.
The governing board must ensure 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 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 their safeguarding needs.

The governor who oversees online safety is the Safeguarding Governor.
All governors will:

- Ensure 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 3)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

3.2 & 3.3 The Head Teacher & Designated safeguarding lead (DSL)
The Head Teacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The Headteacher (DSL) will:

- Work with the governing body to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly.
- Take the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks.
- Work with the ICT manager to make sure the appropriate systems and processes are in place.
- Work with the ICT manager and other staff, as necessary, to address any online safety issues or incidents.
- Manage all online safety issues and incidents in line with the school's child protection policy.
- Ensure that any online safety incidents are logged (see appendix 6) and dealt with appropriately in line with this policy.
- Ensure that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy.
- Update and deliver staff training on online safety (appendix 5 contains a self-audit for staff on online safety training needs).
- Liaise with other agencies and/or external services if necessary.
- Provide regular reports on online safety in school to the governing body.
- Undertake annual risk assessments that consider and reflect the risks children face
- Provide regular safeguarding and child protection updates, including online safety, to all staff, at least annually, to continue to provide them with relevant skills and knowledge to safeguard effectively.

This list is not intended to be exhaustive.

3.4 The Online Safety lead

The Online Safety lead 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 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
  Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- Ensuring that any online safety incidents are logged (see appendix 6) 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.

3.5 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 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- 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 reporting this to the DSL.
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 6) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about 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.

Staff are responsible for the safety of their device by ensuring that it is locked if away from it and left inactive for a period.

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

The school will take every opportunity to help parents and carers understand these issues through:

- Publishing the school Online Safety Policy on the school website.
- Providing them with a copy of the learners' acceptable use agreement.
- Seeking their permissions concerning digital images of children.

- Providing training on the measures they can take to promote safe internet use at home.
- Discuss any concerns related to Online Safety during parents evening.

Parents and carers will be encouraged to support the school in:
- Ensure 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) on Arbor
- Reinforcing the online safety messages provided to learners in school.
- Supporting pupils with use of their children's personal device.
- Not using their personal mobile phones when in the school building
- Respecting the school rules regarding social media postage and not posting photos of children on social media if they contain image of other children by signing the parent acceptable user agreement in appendix 4 on Arbor

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
• Hot topics – Childnet
• Parent resource sheet – Childnet

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 3).

4 Educating pupils about online safety

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

All schools have to teach: Relationships education and health education in primary 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

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/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.

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 and who from the school (if anyone) their child will be interacting with online
- If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the Head teacher (DSL)

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

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. (See also the school behaviour policy.)

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. Class teachers will discuss cyber-bullying with their classes as part of the planned curriculum.

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 (see section 11 for more detail).

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 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 headteacher 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.

6.3 Examining electronic devices
All searches will be conducted in accordance with the DfE guidance Searching, screening and confiscation.

The Head Teacher, and any member of staff authorised to do so by the Head Teacher can carry out 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:

- Assess 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 Head Teacher.
  Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to seek pupil cooperation.

If inappropriate material is found on the device, it is up to Federation Head Teacher 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 if 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 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.

6.4 Artificial Intelligence (AI)

Generative artificial intelligence (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 Bard.

St. Andrew's 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. Crossways will treat any use of AI to bully pupils in line with our anti-bullying and behaviour policies.
Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school.

7 Acceptable uses 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 to 3). 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 to 3.**

8 Technology & Devices

We recognise the importance of cultivating responsible and secure digital practices to protect staff and students. This section outlines our approach to the use of school technology and devices, encompassing a comprehensive set of guidelines and policies designed to create a safe, respectful, and enriching digital environment for all members of our school community.

8.1 Mobile Devices

- All staff who work directly with children should leave their mobile phones on silent and only use them in private staff areas during school hours. Children/staff data should never be downloaded onto a private phone.
- Parents are asked to leave their phones in their pockets and turned off when they are on site. They should ask permission before taking any photos, e.g. of displays in corridors or classrooms, and avoid capturing other children.
- Pupils in Year 5/6 may bring mobile devices into school, but these are handed in to the class teacher on arrival into school, locked in a secure space within the classroom for the school day and returned
  to the children at the end of the day. Children are not permitted to use them during the school day, unless in exceptional circumstances agreed by the Head Teacher/DSL. 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.

8.2 School Devices outside of school

All staff members will take appropriate steps to ensure school devices remain secure when granted permission to use off site. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol).
- Making sure the device locks if left inactive for a period
- Not sharing the device among family or friends.
- Keeping operating systems up to date – always install 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 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 Online Safety Lead.
The school will ensure that work devices:

- Have an encrypted hard drive – 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
- Have anti-virus and anti-spyware software installed

8.3 Photography of students

When a pupil joins the school, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos, for what purpose (beyond internal assessment, which does not require express consent) and for how long using parental consents on Arbor. These can be updated by parents at any time.

- Whenever a photo or video is taken, the member of staff will check the latest database on Arbor before using it for any purpose.
- Any pupils shown in public facing materials are never identified with more than first name (and photo file names/tags do not include full names to avoid accidentally sharing them).
- All staff are governed by their contract of employment and the school's Acceptable Use Policy, which covers the use of mobile phones/personal equipment for taking pictures of

pupils, and where these are stored. Staff will not use their personal phones to capture photos of students.

- Photos are stored on the school network in line with the retention schedule of the school Data Protection Policy
- Staff and parents are reminded annually about the importance of not sharing without permission, due to reasons of child protection (e.g. looked-after children often have restrictions for their own protection), data protection, religious or cultural reasons, or simply for reasons of personal privacy.
- We encourage young people to think about their online reputation and digital footprint, so we should be good adult role models by not oversharing (or providing embarrassment in later life – and it is not for us to judge what is embarrassing or not).
- Pupils are taught about how images can be manipulated in their online safety education programme and taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children.
- Pupils are advised to be very careful about placing any personal photos on social media.
- They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission.
- We teach students about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location.
- We also teach them about the need to keep their data secure and what to do if they or a friend is subject to bullying or abuse.

9 How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and ICT and internet acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

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.

10 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).

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 and DDSLs 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 about 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.

11 Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 6.

This policy will be reviewed every year by the Online Safety Lead. 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.

Appendix 1: EYFS & KS1 acceptable use agreement (pupils & parents/ carers)

<table>
<tr><th colspan="2">ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET:
AGREEMENT FOR PUPILS AND PARENTS/CARERS</th></tr>
<tr><td colspan="2">NAME OF PUPIL:</td></tr>
<tr><td colspan="2">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:
1. I select a website by mistake
2. I receive messages from people I don't know
3. I find anything that may upset or harm me or my friends

• 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.</td></tr>
<tr><td>SIGNED (PUPIL):</td><td>DATE:</td></tr>
<tr><td colspan="2">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.</td></tr>
<tr><td>SIGNED (PARENT/CARER):</td><td>DATE:</td></tr>
</table>

Appendix 2: KS2 acceptable use agreement (pupils and parents/carers)

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

NAME OF PUPIL:

I will read and follow the rules in the acceptable use agreement policy.

- When I use the school's ICT systems (like computers) and the internet in school I will:
- Always use the school's ICT systems and the internet responsibly
- Only use them when a teacher is present, or with a teacher's permission
- Keep my usernames and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or sensible adult) immediately if I find any material that might upset, distress or harm me or others
- Always log off or shut down a computer when I've finished working on it

I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- 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
- Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate
- Log in to the school's network using someone else's details
- 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 hand it to a teacher when I arrive at school and not use it during lessons, 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 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 3: Acceptable use agreement (staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS	
NAME OF STAFF MEMBER/GOVERNOR/ VOLUNTEER/VISITOR:	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way that could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Take photographs of pupils without checking with teachers first Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school	
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me, they have found any material that 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:	**DATE:**

Appendix 4: acceptable use agreement (Parents/ carers)

<table>
<tr><th colspan="2">PARENT/CARER ACCEPTABLE USE AGREEMENT</th></tr>
<tr><td colspan="2">NAME OF PARENT:</td></tr>
<tr><td colspan="2">

I understand that Parent/carers play a crucial role in ensuring that their children understand the need to use the online services and devices in an appropriate way
I will ensure that my child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2) and will sign the agreement on Arbor to allow them to use the internet in school
I will ensure that my wishes regarding the use of digital images of my children are kept up to date on Arbor
I will support the school by promoting safe and responsible use of the internet, online services and digital technology at home. I will inform the school if I have any concerns
I understand that when I visit school I will be asked to leave my phone/mobile device in my pocket and have it turned off when I am on site.
During assemblies, sports events or performances I agree that if I take photos or recordings of my child which includes other children I will:

1. Use these for personal and family use only
2. Not publish photos of my child/children taken at school on social media networks if they contain recognisable images of other children
</td></tr>
<tr><td>SIGNED (PARENT):</td><td>DATE:</td></tr>
</table>

Appendix 5: Online safety training needs – self- audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
NAME:	**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 abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern?	
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?	

Appendix 6: Online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date:	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name & signature of staff member recording**