Version [2.0]

September 2025

ONLINE SAFETY POLICY

Sandon Primary Academy

Mrs R Beckett & Mrs L Kiddle (Co-Principals)

Review date: September 2026

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and Trustees
- 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
- 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, misinformation, disinformation and conspiracy theories (updated in line with KCSIE 2025).
- 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; 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 Principals and school staff
- Searching, screening and confiscation
- Filtering, monitoring and use of AI.

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 Online Safety Act 2023 is also reflected as well as the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The Trustee board

The Trustees have overall responsibility for monitoring this policy and holding the Principal to account for its implementation.

The Trustees will make sure all staff undergo cyber security training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring and the use of AI.

The Trustees 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 Trustees should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The Trustees 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 those 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 Trustees who oversees online safety is Pete

Harbron.

All Trustees 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- ACCEPTABLE USE OF IT | Sandon
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school approach to safeguarding and related policies and procedures

3.2 The Principal

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

3.3 The Designated Safeguarding Lead

The Schools Designated Safeguarding Lead is Kate Burrows and Deputy is Mel Lear

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

- Supporting the Principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Principal and Trust board to review this policy annually and ensure 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
- Working with the lead for computing to make sure the appropriate systems and processes are in place
- Working with the Principal, lead for computing 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
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Principal and/or governing board
- Undertaking annual risk assessments that consider and

reflect the risks children face

3.4 The Lead for Computing

The lead for computing 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 on a weekly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

3.5 Staff

Staff 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 ACCEPTABLE USE OF IT | Sandon
- 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
- Following the correct procedures if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

3.6 Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the Principal of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet ACCEPTABLE USE OF IT | Sandon
- Alerting staff to any online concerns.

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.

4. Educating pupils about online safety

Online safety is delivered to our pupils in multiple ways across the academy. The main way in which this is taught is as part of the progressive computing curriculum which is delivered from EYFS through to Year 6. Within the computing curriculum, online safety is taught throughout sessions. Additionally, the academy participates in key computing dates, such as ‘safer internet day’. The Computing curriculum has been designed to allow for online safety to be taught within Computing lessons and these links have been identified on medium-term planning documents and outlined on the online safety curriculum to ensure appropriate coverage. To support this further, termly online safety assemblies are held across the academy with follow-up discussions and activities being held in classes.

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

In **EYFS,** pupils will be taught to:

- Identify rules that keep us safe
- Identify how people can be unkind online
- Give examples of information that can be put onto the internet and how it can be out on.
-

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
- Understand how other people can see online information

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 staff

All new staff members will receive cyber security training as part of their induction which will then be renewed every 3 years. The induction will also include training 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, 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 deputy 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.

6. Educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety via weekly dojo posts which share age restrictions and guidance documents. Interested parents will be directed to SKIPS courses or referred to referred to organisations such as: Parent info http://parentinfo.org/ Think U Know https://www.thinkuknow.co.uk/

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

7. Cyber-bullying

7.1 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 1 person or group by another person or group, where the relationship involves an imbalance of power (See also the school behaviour policy.)

7.2 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.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes RSHE education, and other subjects where appropriate.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal offences have occurred, 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.

Offences include:

-cyberfishing

-epilepsy trolling

-threatening communication

-encouraging serious self-harm

-sharing intimate images

The school will follow the cyber security standards for school to help improve resilience against cyber-attacks.

7.3 Examining electronic devices

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

- Poses a risk to staff or pupils,

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 Principal and DSL
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

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 DSL / Principal / other member of the senior leadership team 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 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.

7.4 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access.

Sandon Primary Academy 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.

Sandon Primary Academy will treat any use of AI to bully pupils in line with our anti bullying and behaviour policy. If AI is used to create and share sexual images then this is an offence and will be reported to the police following

school safeguarding procedures.

The school has created an AI policy for staff to follow to support them in the safe use of AI to support learning and will work to follow DfE guidance on Generative AI: product safety expectations.

8. Acceptable use of the internet in school

All pupils, parents/carers, staff, volunteers and Trustees are expected to read and agree to an agreement regarding the acceptable use of the school's ICT systems and the internet ACCEPTABLE USE OF IT | Sandon

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, Trustees and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

Internet access is monitored by Laptop House who provide external IT support, the school's ICT Manger (Mr S Griffin), the computing lead (Mr Kiddle) and DSL (Mrs Burrows) who all have access to the school's filtering of inappropriate sites and regularly monitor this. Alerts are sent to the appropriate members of staff to make them aware of any inappropriate use of the internet immediately and these circumstances are looked into accordingly.

How will the risks be assessed?

The school will take all reasonable precautions as outlined above to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access. If staff or pupils discover unsuitable sites, the URL (address) and content must be reported the ICT Manger (Mr Griffin). The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990. Methods to identify, assess and minimise risks will be reviewed regularly with support from the local authority.

9. Acceptable use of emails in school

- Pupils may send e-mails as part of planned lessons.
    - Pupils must not reveal details of themselves or others in e-mail communication, such as address or telephone number, or arrange to meet anyone.
- Pupils and staff must immediately report if they receive an offensive e-mail.
- Pupils and staff must not open attachments from unknown sources- Pupils will be taught this.
- In-coming and out-going e-mails will be regarded as public and may be monitored to maintain the safety of pupils.

10. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them during the school day. Pupils can bring mobile devices into out of school club but an agreement for this usage is singed prior to this. Mobile devices will not be permitted for use on educational visits.

11. Staff using mobile devices in school

- Staff are not permitted to make/receive calls/texts during contact time with children. Emergency contact should be made via the school office.
- Staff are not permitted to take photos or recordings or use any recording software with their personal devices- Should there be exceptional circumstances, then staff should make the principal aware.
- All staff must password protect their mobile device.

12. 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 at least 12 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

of time › Not sharing the device among family or friends

- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates
- Keeping devices secure-not leaving them in a car.

Staff members must not use the device in any way that would violate the school's terms of acceptable use.

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 school's computing lead

13. How the school will respond to issues of misuse.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

14. Website Content

- The point of contact on the Website is the school address, school E-mail and telephone number.
- Staff or pupils' home information will not be published.
- Photographs that are uploaded onto the school website will be carefully selected and will only include photos of pupils whom have parental permission for their photographs to be used/ published.
- Pupils' first names will only be used on the Website and names will not be put with photographs of children.

15. Engaging with Parents through the internet

Information regarding learning activities and school activities is shared with all parents and carers via school's own Facebook page. In the internet usage agreement parents agree that the information and pictures shared on the platform are for their personal use only and should not be shared on social media sites.

16. Managing emerging technology use

The school have examined and will continue to examine the educational benefit of new devices before use in school is allowed.

From observing in other schools and engaging in CPD Sandon Primary have examined the educational benefit of using pupil and staff IPADS as a teaching tool. All staff and pupils from Year 2 upwards will use an IPAD device across the curriculum. These will be used in line with this online safety policy and an additional ipad usage agreement.

17. Social Media

The academy will block/filter pupil access to social media sites.

Pupils and staff will be advised never to give out personal details of any kind which may identify them or their location.

18. Maintaining security of ICT systems

- The school ICT systems will be reviewed regularly with regard to security.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the Laptop House and the trustee who leads on cyber security.
- All portable devices such as memory sticks and SD cards must have multi factor authentication.
- Portable media may not be brought into school without specific permission and a virus check.
- When personal data held on school systems or devices is no longer needed, it must be deleted.
- Emails are to be sent confidentially.
    - Devices are password protected with 12 characters.

19. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety via cpoms.

This policy will be reviewed every year by the DSL.

20. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy
- AI Policy

Acceptable use agreement (staff, trustees, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, TRUSTEES, VOLUNTEERS AND 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 personal social networking sites or chat rooms. • Not share information that links to school on my personal social networking sites. • 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 and class permission lists first and obtaining written consent where needed. • Ensure any photographs taken are only done so on a school device that is secure- Delete pictures once they have been used for their intended and agreed purpose. • 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 • Use public Wi-Fi for accessing sensitive school data unless I am using the school VPN. •	
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 continuously monitor the websites I visit and my use of the school's ICT facilities and systems through their filtering and monitoring system. 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-as located on the school website. I will ensure that my device is locked when I am away from it. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too. I will only use the platform DOJO for online communication with parents.	
If any area of the above agreement is breached this could result in disciplinary proceedings being followed.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Online Communication & ICT Use: Important Guidelines

Parents

We understand that online channels are an important way for parents and carers to communicate with, or about, our school. To ensure a positive and respectful environment, please take note of the following:

Official School Communication Channels

- Facebook: Our official school page
- Class Dojo: Main and class stories

When Communicating with the School

✓ Be respectful towards staff, parents, and pupils at all times
✓ Raise concerns or complaints through the school's official channels, following our complaints procedure

✕ Parents must not:

- Use private groups, the school's Facebook or Dojo pages, or personal social media to complain about or criticise staff or the school. Concerns should be raised privately through teachers, SLT, or our complaints policy.
- Use social media to discuss behaviour issues involving other pupils—please contact the school directly.
- Upload or share photos or videos of children other than your own without parental consent.

Pupil ICT & Internet Use in School

IT is an integral part of school learning with technology utilised in the teaching of all subjects.

To keep pupils safe online, they must:

✓ Always ask a teacher before using laptops or iPads
✓ Only visit appropriate websites
✓ Tell a teacher immediately if they see something upsetting or inappropriate
✓ Use technology responsibly

✕ Pupils must not:

- Go on social media (unless instructed as part of a lesson)
- Use chat rooms or open unknown emails/links
- Use mean or rude language online
- Share inappropriate photos, videos, or livestreams
- Share passwords or log in under someone else's name
- Use AI tools (e.g., ChatGPT, Google Bard) to create and submit work as their own
- Access & use materials related to violent extremism

Parental Responsibility

Parents are expected to discuss these guidelines with their child to support safe and responsible ICT use.
Thank you for your support in maintaining a respectful, safe, and positive online environment for everyone.

Sandon Primary Academy iPad Curriculum:

In school, iPad Use and Responsibility Agreement for Pupils

Purpose of Agreement:

This agreement outlines the responsibilities and expectations related to the use of school-provided iPads for educational purposes as part of the iPad curriculum. It ensures that both students and parents understand the rules for use and accept liability for intentional damage.

Terms and Conditions:

1. **Use of iPad**
   - The iPad is provided by the school for educational use within school only.
   - Pupils must follow the school's acceptable use policy while using the device https://www.sandonprimaryacademy.com/acceptable-use-of-it
   - The iPad must be used respectfully, responsibly, and safely at all times.

2. **Care and Maintenance**
   - Pupils must take proper care of the iPad at all times. The school has purchased high quality cases for every pupil to support them in meeting this action.
   - iPads must be stored securely when not in use. The school has purchased, high quality storage for every iPad to support pupils with this action.
   - No unauthorised software, apps, or modifications may be installed.

3. **Damage, Loss, or Theft**
   - The iPad is expected to remain in the same condition it was issued (reasonable wear and tear expected).
   - All damage must be reported immediately to the teacher or school IT staff.
   - In cases of accidental damage, the school may cover part or all of the cost depending on the circumstances.
   - In cases of **deliberate or negligent damage**, **parents/carers agree to pay for the full cost of repair or replacement**.

4. **Return of Device**
   - The iPad remains the property of the school and must remain within school unless a personalised agreement is made in addition to this agreement.

Acknowledgement and Agreement

I, the Parent/Carer of ……understand and agree to the terms outlined in this agreement. I give permission for my child to use a school-issued iPad as part of the iPad curriculum for educational purposes within school. I also acknowledge and accept responsibility for any **deliberate or negligent damage** caused by my child and agree to pay the costs associated with repair or replacement if required.

Parent/carer Signature: _____ **Date:** _____

Student Signature: _____ **Date:** _____

School Representative Signature: _____ **Date:** _____