THE COOMBES
CE Primary School

'A farmer went to sow his seeds' (Mark 4 3-8)

KEYS Academy Trust

"Unlocking the Future"

TKAT Online Safety Policy

Policy Level and Description:	3	TKAT Policy Guidance Schools may use this to inform the drafting of their non-statutory policy	
Reviewed by: ***(Trust Officer)***	Alex Powley, Director of Teaching and Learning	**Reviewed by:** ***(School representative)***	L Henderson Headteacher
Approved by: ***(Trust Committee/Trust Board)***	CECE	**Approved by:** ***(LGB/LGB Committee)***	LGB
Trust approval date: ***(dd/mm/yyyy)***	15/11/24	**LGB/LGB Committee approval date:** ***(dd/mm/yyyy)***	2.12.2024
Review due: ***(mm/yyyy)***	11/2026		

Version	DATE	DESCRIPTION
Version 1	September 2017	Data and e-safety policy
Version 2	November 2022	Amendment to update policy and reflect changes in Broadband provider
Version 3	September 2023	Change of name to Online Safety Policy and updated to reflect the changes in Keeping Children Safe in Education September 2023
Version 4	November 2024	Added section on artificial intelligence (AI) (6.4) including a reference to deepfake technology Updated section (9) on pupils' use of mobile devices at school.

Contents

Contents

This is a Trust policy to be implemented by all schools within The Keys Academy Trust to ensure a consistent approach for all.

We are a family of distinctive schools at the heart of the diverse communities we serve. In line with our Christian ethos, we aspire to excellent learning and pastoral care for pupils and staff and are committed to being open and welcoming to all.

1. Aims

The aim of this policy is to describe how the school will ensure the safety of pupils whilst using the internet and associated technologies. 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.

This policy complies with our funding agreement and articles of association.

The 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 phones and other personal devices, such as tablets and smart watches.
- 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. Introduction

The Keys Academy Trust believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all pupils and staff are protected from potential harm online. The Keys Academy Trust identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life. The Keys Academy Trust believes that pupils should be empowered to build resilience and to develop strategies to manage and respond to risk online.

This policy applies to all staff including the trustees, governing body, leadership team, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of our schools (collectively referred to as "staff" in this policy) as well as pupils, parents and carers.

This policy applies to all access to the internet and use of technology, including personal devices, or where pupils, staff or other individuals have been provided with school issued devices for use off-site, such as work laptops, tablets or mobile phones.

The school's Data & Online Safety policy will operate in conjunction with other policies including those for Behaviour, Disciplinary, Anti- Bullying, Curriculum and Data Protection.

Our Online Safety Policy has been written by the Trust, following guidance from Wokingham Borough Council, The Key and government guidance. It has been agreed by the senior leadership team and approved by the governors.

3. Roles and responsibilities

3.1 The local governing body

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

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

The Local Governing Body 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.

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 The Senior Leadership Team

The Senior Leadership Team is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school. The Senior Leadership Team will:

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Ensure there are appropriate and up-to-date policies regarding online safety; including a staff code of conduct/behaviour policy and acceptable use policy, which covers acceptable use of technology.
- Ensure that suitable and appropriate filtering and monitoring systems are in place and work with technical staff to monitor the safety and security of our systems and networks.
- Ensure that online safety is embedded within a progressive curriculum, which enables all pupils to develop an age-appropriate understanding of online safety.
- Support the DSL and any deputies by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.
- Ensure there are robust reporting channels for the community to access regarding online safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology.
- Audit and evaluate online safety practice to identify strengths and areas for improvement.

3.3 The Designated Safeguarding Lead

Details of the school's designated safeguarding lead (DSL) and deputy/deputies are set out in the child protection and safeguarding policy, as well as relevant job descriptions.

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

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the headteacher and the Local Governing Body 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 ICT manager to make sure the appropriate systems and processes are in place.
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents.
- Managing all online safety issues and incidents in line with the school's child protection policy.
- Ensuring that any online safety incidents are logged (see appendix 5) 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 (appendix 4 contains a self-audit for staff on online safety training needs).

- Liaising with other agencies and/or external services if necessary.
- Providing regular reports on online safety in school to the headteacher and/or Local Governing Body.
- Undertaking annual risk assessments that consider and reflect the risks children face.
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively.

3.4 The ICT Manager

The ICT manager is responsible for:

- Provide technical support and perspective to the DSL and Senior Leadership Team, especially in the development and implementation of appropriate online safety policies and procedures.
- 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 monthly basis.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- Ensure appropriate access and technical support is given to the DSL (and/or deputy) to the school's filtering and monitoring systems, to enable them to take appropriate safeguarding action if/when required.
- Ensuring that any online safety incidents are logged (see appendix 5) 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 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.

- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) 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'
- Taking responsibility for the security of setting systems and the data they use or have access to.
- Modelling good practice when using technology and maintaining a professional level of conduct in their personal use of technology, both on and off site.
- Embedding online safety education in curriculum delivery, wherever possible.
- Having an awareness of a range of online safety issues and how they may be experienced by the children in their care.
- Taking personal responsibility for professional development in this area.

3.6 Pupils

It is the responsibility of pupils (at a level that is appropriate to their individual age and ability) in our schools to:

- Engage in age-appropriate online safety education opportunities.
- Contribute to the development of online safety policies.
- Read and adhere to the acceptable use policies.
- Respect the feelings and rights of others both on and offline.
- Take responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if there is a concern online, and support others who may be experiencing online safety issues.

3.7 Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher 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 (appendices 1 and 2)
- Support our online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home.
- Model safe and appropriate use of technology and social media.
- Abide by the home-school agreement and acceptable use policies.
- Identify changes in behaviour that could indicate that their child is at risk of harm online.

- Seek help and support from the school, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Contribute to the development of the online safety policies. Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

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 International
- Parent resource sheet – Childnet International

3.8 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 primary 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 search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content.
- 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.

Our schools will support pupils to read and understand the acceptable use policies in a way which suits their age and ability by:

- Displaying acceptable use posters in all rooms with internet access.
- Informing pupils that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
- Rewarding positive use of technology in accordance with their Behaviour Policy.
- Providing online safety education and training as part of the transition programme across the key stages and when moving between establishments.
- Seeking learner voice when writing and developing online safety policies and practices, including curriculum development and implementation.
- Using support, such as external visitors, where appropriate, to complement and support our internal online safety education approaches.

4.1 Vulnerable Pupils

The Keys Academy Trust recognises that some pupils are more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.

Our schools will ensure that access to appropriately adapted online safety education materials and support is provided to vulnerable pupils.

When seeking to adapt the online safety curriculum our schools will seek input from specialist staff as appropriate, including the SENCO and Child in Care Designated Teacher.

4.2 Training and engagement with staff

Our schools will:

- Provide and discuss the online safety policy and procedures with all members of staff as part of induction.

- Provide up-to-date and appropriate online safety training for all staff on a regular basis, with at least annual updates as part of existing safeguarding and child protection training. This will cover the potential risks posed to pupils (Content, Contact and Conduct) as well as our professional practice expectations.
- Recognise the expertise staff build by undertaking safeguarding training and managing safeguarding concerns and provide opportunities for staff to contribute to and shape online safety policies and procedures.
- Make staff aware that our IT systems are monitored, and that activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices.
- Make staff aware that their online conduct outside of the setting, including personal use of social media, could have an impact on their professional role and reputation.
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the pupils.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting pupils, colleagues or other members of the community.

5. Educating parents/carers about online safety

The Keys Academy Trust recognises that parents and carers have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies.

Our schools will build a partnership approach to online safety with parents and carers by:

- Providing information and guidance on online safety in a variety of formats.
    - This will include offering specific online safety awareness training and highlighting online safety at other events such as parent evenings, transition events, fetes and sports days.
- Drawing their attention to the online safety policy and expectations in newsletters, letters, school prospectus and on the school's website.
- Requesting that they read online safety information as part of joining the school community, for example, within the school's home school agreement.
- Requiring them to read our acceptable use policies and discuss the implications with their children.
- Making advice on filtering systems and educational and leisure activities that include responsible use of the Internet available to parents via the Online Safety link on our learning platform.

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 headteacher and/or the DSL.

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

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the 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.)

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.

Our schools will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class Teachers will discuss cyber-bullying with their classes.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

Our schools also send 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, each school will follow the processes set out in their school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will 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

The headteacher, and any member of staff authorised to do so by the headteacher, 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 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 Head Teacher or 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 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 Head Teacher and/or DSL 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
- The school's behaviour policy

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.

The Keys Academy Trust 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.

Our schools will treat any use of AI to bully pupils in line with their anti-bullying/behaviour policy.

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. Social Media

7.1 Expectations

The expectations' regarding safe and responsible use of social media applies to all members in all of our school communities.

The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messengers.

All members of our community within our schools are expected to engage in social media in a positive, safe and responsible manner.

All members of our communities within our schools are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.

The schools will control learner and staff access to social media whilst using setting provided devices and systems on site.

The use of social media during school hours for personal use is not permitted.

Inappropriate or excessive use of social media during school hours or whilst using school devices may result in disciplinary or legal action and/or removal of internet facilities.

Concerns regarding the online conduct of any member within our school communities on social media, should be reported to the DSL within the specific school and will be managed in accordance with our anti-bullying, allegations against staff, behaviour and child protection policies.

7.2 Staff Personal Use of Social Media

The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.

Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of our code of conduct policy as part of acceptable use policy.

All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the setting.

Civil, legal or disciplinary action may be taken if staff are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

All members of staff are advised to safeguard themselves and their privacy when using social media sites. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include (but is not limited to):

- Configuring appropriate privacy settings on their social media profiles
- Being aware of location sharing services.
- Opting out of public listings on social networking sites.
- Logging out of accounts after use.
- Keeping passwords safe and confidential.
- Ensuring staff do not represent their personal views as that of the school.

Members of staff are encouraged not to identify themselves as employees of any of the schools within The Keys Academy Trust on their personal social networking accounts; this is to prevent information on these sites from being linked with the setting, and to safeguard the privacy of staff members.

All members of staff are encouraged carefully to consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance our policies and the wider professional and legal framework.
Information and content that staff members have access to as part of their employment, including photos and personal information about pupils and their family members or colleagues will not be shared or discussed on social media sites.

Members of staff will notify the Leadership Team immediately if they consider that any content shared on social media sites conflicts with their role.

7.3 Communicating with Pupils and Parents and Carers

All members of staff are advised not to communicate with or add as ‘friends’ any current or past pupils or their family members via any personal social media sites, applications or profiles.

Any pre-existing relationships or exceptions that may compromise this, will be discussed with school’s DSL (or deputy) and/or the Head Teacher.

Staff will not use personal social media accounts to contact pupils or parents, nor should any contact be accepted.

Any communication from pupils and parents received on personal social media accounts will be reported to the DSL (or deputy).

7.4 Pupils' Personal Use of Social Media

Safe and appropriate use of social media will be taught to pupils as part of an embedded and progressive education approach, via age-appropriate sites and resources.

Any concerns regarding pupils' use of social media will be dealt with in accordance with existing policies, including anti-bullying and behaviour policies.

Concerns will be shared with parents/carers as appropriate, particularly when concerning underage use of social media sites, games or tools.

Pupils will be advised:

- To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location.
- To only approve and invite known friends on social media sites and to deny access to others by making profiles private.
- Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.
- To use safe passwords.
- To use social media sites which are appropriate for their age and abilities.
- How to block and report unwanted communications.
- How to report concerns both within the setting and externally.

7.4 Official Use of Social Media

The Coombes CE Primary School official social media channels are:
Twitter link @Coombes_School

The official use of social media sites only takes place with clear educational or community engagement objectives, with specific intended outcomes. The official use of social media as a communication tool has been formally risk-assessed and approved by the headteacher. Leadership staff have access to account information and login details for our social media channels, in case of emergency, such as staff absence.

Official social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only. Staff use setting-provided email addresses to register for and manage any official social media channels. Official social media sites are suitably protected and, where possible, run *and/or* linked *to/from* the school's website. Public communications on behalf of the setting will, where appropriate and possible, be read and agreed by at least one other colleague.

Official social media use will be conducted in line with existing policies, including: anti-bullying, image/camera use, data protection, confidentiality and child protection policies. All communication on official social media platforms will be clear, transparent and open to scrutiny.

Parents/carers and pupils will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community. Only social media tools which have been risk assessed and approved as suitable for educational purposes will be used.

Parents and carers will be informed of any official social media use with pupils; written parental consent will be obtained, as required.

Our schools will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

7.5 Staff expectations

Members of staff who follow and/or like school official social media channels will be advised to use dedicated professionals accounts, where possible, to avoid blurring professional boundaries.

If members of staff are participating in online social media activity as part of their capacity as an employee of the Trust, they will:

- Sign our social media acceptable use policy.
- Always be professional and aware they are an ambassador for the Trust.
- Disclose their official role *and/or* position but make it clear that they do not necessarily speak on behalf of the Trust.
- Always be responsible, credible, fair and honest, and consider how the information being published could be perceived or shared.
- Always act within the legal frameworks they would adhere to within the workplace, including: libel, defamation, confidentiality, copyright, data protection and equalities laws.
- Ensure that they have appropriate consent before sharing images on the official social media channel.
- Not disclose information, make commitments or engage in activities on behalf of the Trust, unless they are authorised to do so.
- Not engage with any direct or private messaging with current, or past, pupils, parents and carers.
- Inform their line manager, the DSL (or deputy) and/or the Head Teacher of any concerns, such as criticism, inappropriate content or contact from pupils.

8. Acceptable Use of the Internet in School

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 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.

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

More information is set out in the acceptable use agreements in appendices 1 to 3.

9. Pupils Using Mobile Devices in School

There may be specific circumstances under which a pupil needs to bring a mobile phone to school, for instance:

• parent/carer expectations

• if they are travelling to school by themselves

• are part of certain groups of pupils (such as young carers) that may need access to a mobile

• behaviour or safeguarding risks which may require access to a mobile phone

Pupils who are allowed to bring mobile phones to school must hand in their phone to the class teacher/school office (amend as necessary for your school) who will store them securely during the school day.

They must not have them in classrooms or on their person and must not use them on the school's premises, including the playground or school field.

Apart from specific circumstances agreed with senior leaders, children should not have mobile phones in school. Other recording devices such as smart watches which may have a camera or connectivity should not be brought into school.

For further information, please refer to the TKAT Mobile Phone policy.

10. 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 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol).
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device.
- Making sure the device locks if left inactive for a period of time.

- Not sharing the device among family or friends.
- Installing anti-virus and anti-spyware software.
- Keeping operating systems up to date by always installing the latest updates

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

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, Schools will follow the procedures set out in their 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 disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

Incidents that involve illegal activity or content, or otherwise serious incidents will be reported to the police.

11. 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, 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 deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring arrangements

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

This policy will be reviewed every year by the Keys Academy Trust. At every review, the policy will be shared with Trustees. 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:

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

Appendix A – Classroom use of Technology

Classroom Use

Our schools use a wide range of technology. This includes access to:

- *Computers, laptops, tablets and other digital devices*
- *Internet which may include search engines and educational websites*
- *Learning platform*
- *Email*
- *Digital cameras, web cams and video cameras*

All school-owned devices will be used in accordance with our acceptable use policies and with appropriate safety and security measures in place. Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home. The school will use age-appropriate search tools following an informed risk assessment, to identify which tool best suits the needs of our community.

The Keys Academy Trust advises that the following search engines are used:

- *SWGfL Swiggle*
- *Dorling Kindersley find out*
- *Google Safe Search*
- *School created Google custom searches*
- KidRex

Schools will ensure that the use of internet-derived materials, by staff and pupils complies with copyright law and acknowledge the source of information.

Supervision of pupils will be appropriate to their age and ability:

- **Early Years Foundation Stage and Key Stage 1**
    - Access to the internet will be by adult demonstration, with occasional directly supervised access to specific and approved online materials, which supports the learning outcomes planned for the pupils age and ability.
- **Key Stage 2**
    - Pupils will use age-appropriate search engines and online tools.
    - Pupils will be directed by the teacher to online materials and resources which support the learning outcomes planned for the pupils' age and ability.

Managing Internet Access

The school will maintain a record of users who are granted access to our devices and systems. All staff, pupils and visitors will read and sign an acceptable use policy before being given access to our computer system, IT resources or internet.

Filtering and Monitoring

Decision Making

The school governors and leaders have ensured that our school has age- and ability-appropriate filtering and monitoring in place, to limit learner's exposure to online risks. The governors and leaders are aware of the need to prevent "over blocking", as that may unreasonably restrict what can be taught, with regards to online activities and safeguarding. Our decision regarding filtering and monitoring has been informed by a risk assessment, considering our specific needs and circumstances. Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from the leadership team; all changes to the filtering policy are logged and recorded. The leadership team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate. All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard pupils; effective classroom management and regular education about safe and responsible use is essential.

Filtering

Education broadband connectivity is provided through Schools Broadband. We use Netsweeper which blocks sites which can be categorised as: pornography, racial hatred, extremism, social networking, gaming and sites of an illegal nature.

The filtering system blocks all sites on the (IWF) list. We work with Schools Broadband. We use Netsweeper to ensure that our filtering policy is continually reviewed. If pupils discover unsuitable sites, they will be required to:

- Turn off the monitor or minimise the window immediately.
- Report the incident to the teacher or responsible adult.

Our teachers should:

- Ensure the well-being of the pupil.
- Note the details of the incident, especially the web page address that was unsuitable (without re-showing the page to the pupils).
- Report the details of the incident to the DSL (or deputy) and/or technical staff.

The DSL will then:

- Log the incident and take any appropriate action.
- Inform parents/carers of filtering breaches involving their child.
- Any material believed to be illegal will be reported immediately to the appropriate agencies, such as the IWF, Police or CEOP.

Monitoring

The school will appropriately monitor internet use on all setting-owned or provided internet enabled devices. This is achieved by:

- Physical monitoring (supervision).
- Monitoring internet and web access (reviewing logfile information).

- Active technology monitoring services provided by NetSupport.
- If a concern is identified via monitoring approaches, the DSL or deputy will respond in line with the child protection policy.
- All users will be informed that use of our systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

Complaints Regarding Internet Use

Our schools have procedures in place for dealing with any complaint of Internet misuse. Complaints of a child protection nature must be dealt with in accordance with school child protection procedures. Pupils and parents will be informed of the school's complaints procedure. Complaints of Internet misuse will be dealt with by the Head Teacher. Any complaint about staff misuse will be referred to the headteacher.

Sanctions

Our schools have a system of sanctions to promote the appropriate use of technology. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990. This would constitute a disciplinary matter as far as staff are concerned.

Managing Personal Data Online

Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations and Data Protection legislation.

Security and Management of Information Systems

The School will take appropriate steps to ensure the security of our information systems, including:

- Virus protection being updated regularly.
- Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
- Not using portable media without specific permission; portable media will be checked by an anti-virus/malware scan before use.
- Not downloading unapproved software to work devices or opening unfamiliar email attachments.
- Regularly checking files held on our network,
- The appropriate use of user logins and passwords to access our network.
    - Specific user logins and passwords will be enforced for all but children in EYFS.
- All users are expected to log off or lock their screens/devices if systems are unattended.
- Further information about technical environment safety and security can be found under our acceptable use policies.

Password policy

All members of staff will have their own unique username and private passwords to access school systems; members of staff are responsible for keeping their passwords private.

All passwords used by adults should follow the guidelines in this policy. No individual should log on using another individual's password, unless they are a member of staff logging on as a child. No individual should tell another individual their password. Once a computer has been used, users must remember to log off so

that others cannot access their information. Users leaving a computer temporarily should lock the screen. Passwords must be changed every school term and must meet complexity requirements. A security setting determines whether passwords meet these requirements. These requirements are enforced when passwords are changed or created. The minimum requirements are that a password must:

- Not contain the user's account name or parts of the user's full name that exceed two consecutive characters.
- Be at least eight characters in length.
- Contain characters from three of the following four categories:
    - English uppercase characters (A through Z)
    - English lowercase characters (a through z)
    - Base 10 digits (0 through 9)
    - Non-alphabetic characters (for example, !, $, #, %)

Passwords must not be easily guessable by anyone. If a password is identified as insecure then it is essential that the password is changed immediately.

Managing the Safety of the School Website

The school will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE). They will ensure that their website complies with guidelines for publications including: accessibility; data protection; respect for intellectual property rights; privacy policies and copyright. Staff or pupils' personal information will not be published on the school website; the contact details on the website will be the school's address, email and telephone number. The administrator account for the school's website will be secured with an appropriately strong password. Our schools will post appropriate information about safeguarding, including online safety, on our website for members of the community.

Publishing Images and Videos Online

The school will ensure that all images and videos shared online are used in accordance with the associated polices, including the: data security policy, acceptable use policies, codes of conduct/behaviour, social media and use of personal devices and mobile phones.

Managing Email

Access to each schools' email systems will always take place in accordance with data protection legislation and in line with other policies, including confidentiality, acceptable use policies and the code of conduct/behaviour policy:

- The forwarding of any chain messages/emails is not permitted.
- Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.

- School email addresses and other official contact details will not be used for setting up personal social media accounts.

Members of the community will immediately tell the DSL (or deputy) if they receive offensive communication, and this will be recorded in the school's safeguarding files/records. Excessive social email use can interfere with teaching and learning and will be restricted; access to external personal email accounts (e.g. Google Mail) may be blocked by the school.

Staff email

The use of personal email addresses by staff in our schools for any official school business is not permitted. All members of staff are provided with an email address to use for all official communication. All of our members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff, pupils and parents.

Pupil email

Pupils in KS2 will use provided email accounts for educational purposes. Pupils will sign an acceptable use policy and will receive education regarding safe and appropriate email etiquette before access is permitted.

Management of Learning Platforms

The schools uses Schools Broadband as its official learning platform. Leaders and staff will regularly monitor the usage of the Learning Platform (LP), including message/communication tools and publishing facilities. Only current members of staff, pupils and parents will have access to the LP.

When staff and/or pupils leave the setting, their account will be disabled and deleted.

Pupils and staff will be advised about acceptable conduct and use when using the LP. All users will be mindful of copyright and will only upload appropriate content onto the LP. Any concerns about content on the LP will be recorded and dealt with in the following ways:

- The user will be asked to remove any material deemed to be inappropriate or offensive.
- If the user does not comply, the material will be removed by the site administrator.
- Access to the LP for the user may be suspended.
- The user will need to discuss the issues with a member of leadership before reinstatement.
- A learner's parents/carers may be informed.
- If the content is illegal, we will respond in line with existing child protection procedures.

Pupils may require editorial approval from a member of staff. This may be given to the pupil to fulfil a specific aim and may have a limited time frame.

A visitor may be invited onto the LP by a member of the leadership team; in this instance, there may be an agreed focus or a limited time slot.

Management of Applications (apps) used to Record Children's Progress

Each school within the Trust uses Target Tracker to track pupils progress and share appropriate information with parents and carers.

The headteacher is ultimately responsible for the security of any data or images held of children. As such, they will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that they are used in accordance with data protection legislation, including the General Data Protection Regulations (GDPR) and Data Protection legislation.

To safeguard pupils' data:

- Only school issued devices will be used for apps that record and store pupils' personal details, attainment or photographs.
- Personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store pupils' personal details, attainment or images.
- Devices will be appropriately encrypted if taken off site, to reduce the risk of a data security breach, in the event of loss or theft.
- All users will be advised regarding safety measures, such as using strong passwords and logging out of systems.
- Parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images.

Appendix 1: EYFS and KS1 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:	

When I use the school's ICT systems (like computers) and get onto the internet in school I will:
• Ask a teacher or adult if I can do so before using them.
• Only use websites that a teacher or adult has told me or allowed me to use.
• Tell my teacher immediately if:
  ○ I click on a website by mistake.
  ○ I receive messages from people I don't know.
  ○ I find anything that may upset or harm me or my friends.
• Use school computers for school work only.
• Be kind to others and not upset or be rude to them.
• Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly.
• Only use the username and password I have been given.
• Try my hardest to remember my username and password.
• Never share my password with anyone, including my friends.
• Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer.
• Save my work on the school network.
• Check with my teacher before I print anything.
• Log off or shut down a computer when I have finished using it.
I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.	

Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 2: 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 get onto the internet in school I will:** • Always use the school's ICT systems and the internet responsibly and for educational purposes only. • 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 which 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 not use it during lessons, break/lunch times, 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's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 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 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 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 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 4: Laptop/Devices Acceptable Use Agreement

1. **Introduction**
   - This agreement applies to all laptops and other associated devices which are loaned to staff and therefore remain the property of the school.
   - It should be read in conjunction with the school's Online Safety Policy
   - All recipients and users of these devices should read and sign the agreement.

2. **Security of equipment and data**
   - The laptop and any other equipment provided should be stored and transported securely. Special care must be taken to protect the laptop and any removable media devices from loss, theft or damage. Users must be able to demonstrate that they took reasonable care to avoid damage or loss.
   - Staff should understand the limitations of the school's insurance cover.
   - Government and school policies regarding appropriate use, data protection, information security, computer misuse and health and safety must be adhered to. It is the user's responsibility to ensure that access to all sensitive information is controlled.

3. **Software**
   - Any additional software loaded onto the laptop should be in connection with the work of the school. No personal software should be loaded.
   - Only software for which the school has an appropriate licence may be loaded onto the laptop. Illegal reproduction of software is subject to civil damages and criminal penalties.
   - Users should not attempt to make changes to the software and settings that might adversely affect its use.

4. **Faults**
   - In the event of a problem with the computer, the school's ICT Technician/Network Manager should be contacted.

Declaration:
I have read and understood the above and also the school's Online Safety Policy and agree to abide by the rules and requirements outlined.

Name:	
Signature:	
Date:	

Appendix 5 Parent/Carer Acceptable Use Agreement

The school seeks to ensure that *students/pupils* have good access to ICT to enhance their learning and, in return, expects *students/pupils* to agree to be responsible users. A copy of the *Student/Pupil* Acceptable Use Agreement is attached to this permission form, so that parents/carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

==========

Acceptance of Use Form

Parent/Carer's Name:	
Student/Pupil's Name:	

As the parent/carer of the above *student/pupil*, I understand that my son/daughter will have access to the internet and to ICT systems at school.

I know that my son/daughter has signed an Acceptable Use Agreement and has received, or will receive, Online Safety education to help them understand the importance of safe use of ICT – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's/daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's Online Safety.

Signature:	
Date:	

Appendix 6: Online Safety Training Needs – Self-Audit For Staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 7: Responding to Incidents of Misuse – Flow Chart