KEYS Academy Trust

"Unlocking the Future"

TKAT Online Safety Policy

Policy Level and Description:	1	TKAT Statutory Policy NO CHANGES TO THE CORE TEXT ALL Schools require a policy on this topic/area. Only changes to highlighted sections are allowed to the core text – changes will be limited to school name and very limited school-specific details - LGBs to adopt, implement and monitor this policy.	
Reviewed by: ***(Trust Officer)***	Alex Powley, Director of Teaching and Learning	**Reviewed by:** ***(School representative)***	Tom Smith, Head of School
Approved by: ***(Trust Committee/Trust Board)***	CECE	**Approved by:** ***(LGB/LGB Committee)***	CDC Committee
Trust approval date: ***(dd/mm/yyyy)***	06/10/2025	**LGB/LGB Committee approval date:** ***(dd/mm/yyyy)***	LGB November 2025
Review due: ***(mm/yyyy)***	10/2026		

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.
Version 5	September 2025	Updated to reflect statutory guidance on RSE, filtering and monitoring, advice for parents/carers, link to AI policy

Contents

Version	Date	Description
1	September 2017	Data and e-safety policy
2	November 2022	Amendment to update policy and reflect changes in Broadband provider
3	September 2023	Change of name to Online Safety Policy and updated to reflect the changes in Keeping Children Safe in Education September 2023
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.
5	October 2025	Reviewed as part of cycle. Updated section on AI and filtering, monitoring and safety features in line with KCSIE 2025.

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

The term 'parent' should be read as 'parent, carer or guardian' throughout.

TKAT vision

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. Introduction

1.1. The Keys Academy Trust (TKAT) 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.

1.2. 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.

1.3. 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.

1.4. 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.

1.5. Our Online Safety Policy has been written by the Trust, following guidance from Wokingham Borough Council, The Key and government guidance. It has approved by Trustees and adopted by all schools in TKAT.

2. Aims and scope

2.1. 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 guidance for schools on the following:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education (RSE) and Relationships and Health Education (RHE)
- Searching, screening and confiscation.

It also refers to the DfE's guidance on protecting children from radicalisation.

2.2. The policy 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.

2.3. The policy also takes into account the National Curriculum computing programmes of study.

2.4. The school aims to achieve the following:

- 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.

2.5. 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, misinformation, disinformation (including fake news), conspiracy theories, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism.
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit 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.

3. Roles and responsibilities

All lists in this section are not intended to be exhaustive.

Trustees

3.1. Trustees have the responsibility for agreeing and approving this policy, and ensuring overall accountability for its implementation, along with the CEO and other senior leaders.

The Local Governing Body (LGB)

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

3.3. 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.

3.4. The Local Governing Body will also make sure all staff receive regular online safety updates as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

3.5. 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).

3.6. The Local Governing Body will make sure that the school teaches pupils how to keep themselves and others safe, including online and when using generative AI (see TKAT AI Policy).

3.7. 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. This includes in relation to generative AI (see TKAT AI Policy). 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 the following:

- 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.

3.8. All governors are responsible for the following:

- Ensure they have read and understand this policy.
- Agree and adhere to set terms on acceptable use of the school's ICT systems and the internet.
- 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.

The Senior Leadership Team

3.9. The Senior Leadership Team (SLT) of each school is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The Designated Safeguarding Lead

3.10. The Designated Safeguarding Lead (DSL) is responsible for the following:

- 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

- Providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly
- Working with the ICT manager to make sure the appropriate systems and processes are in place.
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents.
- Managing all online safety issues and incidents in line with the school's child protection policy.
- Responding to safeguarding concerns identified by filtering and monitoring
- Making sure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy.
- Making sure 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.

The ICT Manager / IT Technical Support

3.11. The ICT manager is responsible for the following:

- The 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.
- Making sure that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Conducting a full security check and monitoring the school's ICT systems on a monthly basis.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- Making sure that any online safety incidents are logged (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.

All Staff and volunteers

3.12. All staff and responsible adults, including contractors and agency staff, and volunteers are responsible for the following:

- 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
- Making sure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'.

Pupils

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

- 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.

Parents

3.14. Parents are expected to support the following:

- Notify a member of staff or the school 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.

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

- What are the issues? UK Safer Internet Centre
- Help and advice for parents/carers Childnet International
- Parent resource sheet Childnet International

Visitors and members of the community

3.16. Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

4. Educating pupils about online safety

4.1. 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.

4.2. In **Key Stage 1**, pupils will be taught the following:

- 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.

4.3. 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.

4.4. 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.

4.5. The safe use of social media and the internet will also be covered in other subjects where relevant.

4.6. Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

5. Educating parents about online safety

5.1. 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.

5.2. Our schools will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.

5.3. The school will let parents 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

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

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

6. Cyber-bullying

Definition

6.1. 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.)

Preventing and addressing cyber-bullying

6.2. 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.

6.3. 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.

6.4. 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.

6.5. 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).

6.6. 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.

6.7. 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.

6.8. The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

Examining electronic devices

6.9. The School Leader, and any member of staff authorised to do so by the School Leader, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting one or more of the following:

- 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.

6.10. Before a search, if the school leader or authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also ensure the following:

- 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.

6.11. 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.

6.12. 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 achieve any of the following:

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

6.13. If inappropriate material is found on the device, it is up to School Leader 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.

6.14. 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 it meets one or more of the following criteria:

- 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.

6.15. 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 ensure the following:

- **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

6.16. 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.

6.17. With regard to AI (see the section entitled 'Artificial Intelligence' within this policy), 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 very seriously, in line with their anti-bullying/behaviour policy.

7. Artificial Intelligence (AI)

7.1. Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents may be familiar with generative AI tools such as ChatGPT and Google Gemini.

7.2. The Keys Academy Trust has a separate Artificial Intelligence Policy; the responsible parties and users outlined within this policy should read the AI Policy as well.

7.3. Any use of artificial intelligence should be carried out in accordance with our TKAT AI Policy.

8. Social Media

8.1 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.

8.2 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.

8.3 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).

8.4 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.

9. Acceptable use of the internet in schools

9.1. All pupils, parents, staff, volunteers and governors are expected to adhere to an agreement regarding the acceptable use of the school's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

9.2. 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.

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

10. Pupils using mobile devices in school

10.1. Each school (in communication with its local governing body) will agree its own procedure and parameters for whether pupils may bring in and/or use mobile devices in school, and clearly explain these expectations to parents and pupils.

10.2. Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

11. Device and use log in safety

11.1. Our IT provider will ensure the below systems are in place. All staff members will take appropriate steps to ensure their devices remain secure, using these systems and processes. This includes, but is not limited to, the following:

- Keeping the device password-protected (in line with guidance) or generated by a password manager.
- Ensure 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

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

11.3. Work devices must be used solely for work activities.

11.4. If staff have any concerns over the security of their device, they must seek advice from their IT Support Provider.

12. How the school will respond to issues of misuse

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

12.2. 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.

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

13. Training

Staff, governors and volunteers

13.1. 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.

13.2. 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).

13.3. 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 the following:

- 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.

13.4. Training will also help staff to ensure the following:
- 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.

13.5. The DSL and 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.

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

13.7. Volunteers will receive appropriate training and updates, if applicable.

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

Pupils

13.9. All pupils will receive age-appropriate training on safe internet use, including the following:
- Methods that hackers use to trick people into disclosing personal information
- Password security
- Social engineering
- The risks of removable storage devices (e.g. USBs)
- Multi-factor authentication
- How to report a cyber incident or attack
- How to report a personal data breach

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

14. Monitoring arrangements

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

14.2. This policy will be reviewed annually 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.

15. Links with other policies

15.1. This online safety policy is linked to the following:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- AI Policy.

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.

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
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 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 5: 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 6: Responding to Incidents of Misuse – Flow Chart