



Online Safety Policy

All changes from the previous version are highlighted in green.

Created by COM April 2024	Ratified by Trustees May 2024
Reviewed January 2025	Ratified by Trustees February 2025
Next review due January 2026	

Contents

Statement of Intent	3
Legal Framework.....	4
Roles and Responsibilities.....	4
Managing Online Safety.....	6
Cyberbullying	8
Child-on-child sexual abuse and harassment	8
Grooming and Exploitation	9
Mental Health	11
Online hoaxes and harmful online challenges.....	11
Cyber-crime.....	12
Online Safety Training for Staff.....	12
Online Safety and the Curriculum.....	13
Use of Technology in the Classroom.....	14
Use of Smart Technology	14
Educating Parents/Carers	15
Internet Access.....	16
Filtering and Monitoring Online Activity.....	16
Network Security	17
Emails	17
Generative Artificial Intelligence (AI).....	18
Social Networking	18
School Website	18
Use of Devices.....	18
Remote Learning.....	19
Monitoring and Review.....	19
APPENDIX A - Online Harms and Risks – Curriculum Coverage	20

Statement of Intent

Keystone Academy Trust understands that using online services is an important aspect of enhancing teaching and learning, promoting pupil achievement, and raising educational standards. The use of online services is embedded throughout the trust; therefore, there are a number of controls in place to ensure the safety of pupils and staff.

The breadth of issues classified within online safety is considerable, but they can be categorised into four areas of risk:

1. **Content:** Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, self-harm and suicide, and discriminatory or extremist views.
2. **Contact:** Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children.
3. **Conduct:** Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.
4. **Commerce:** Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The measures implemented to protect pupils and staff revolve around these areas of risk. The trust has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

Legal Framework

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2024) 'Filtering and monitoring standards for schools and colleges'
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2024) 'Keeping children safe in education 2023'
- DfE (2023) 'Teaching online safety in school'
- DfE (2022) 'Searching, screening and confiscation'
- DfE (2023) 'Generative artificial intelligence in education'
- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2024) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'
- National Cyber Security Centre (2020) 'Small Business Guide: Cyber Security'

This policy operates in conjunction with the following school policies:

- Allegations of Abuse Against Staff Policy
- IT and Devices Acceptable Use Policy
- IT and Devices Acceptable Use Policy (Pupils)
- Cyber Security Policy
- Digital Continuity Statement
- Child Protection and Safeguarding Policy inc Prevent Duty
- Anti-harassment and Bullying Policy
- Staff Code of Conduct
- Pupil Behaviour and Exclusions Policy
- Disciplinary Procedure Policy
- Data Protection Policy

Roles and Responsibilities

The Local Governing Board will be responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the Designated Safeguarding Lead's (DSL) remit covers online safety.
- Reviewing this policy on an annual basis.
- Ensuring their own knowledge of online safety issues is up to date.
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction and at regular intervals.

- Ensuring that there are appropriate filtering and monitoring systems in place.
- Ensuring that the effectiveness of filtering and monitoring systems is reviewed at least annually in liaison with ICT staff and service providers.
- Ensuring that the School Leaders and other relevant staff have an awareness and understanding of the filtering and monitoring provisions in place and manage them effectively and know how to escalate concerns when identified.
- Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.

The headteacher will be responsible for:

- Ensuring that online safety is a running and interrelated theme throughout all the schools' policies and procedures, including in those related to the curriculum, teacher training and safeguarding.
- Supporting the DSL and the Deputy DSL by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.
- Ensuring staff receive regular, up-to-date, and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated. (LCC Safeguarding Audit)
- Organising engagement with parents/carers to keep them up to date with current online safety issues and how each school is keeping pupils safe.
- Working with the DSL and Turn IT On to conduct termly light-touch reviews of this policy.
- Strategic responsibility for online safety in each school.

The DSL will be responsible for or can delegate responsibility for:

- Undertaking training or allocate training to others so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.
- Liaising with relevant colleagues on online safety matters, e.g. leadership team and Turn IT On.
- Ensuring online safety is recognised as part of all schools' safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in each individual school's approach to remote learning.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff, and ensuring all members of the school community understand this procedure.
- Understanding the filtering and monitoring processes in place at the school.
- Ensuring that all safeguarding training given to staff includes an understanding of the expectations, roles and responsibilities in relation to filtering and monitoring systems at the school.
- Maintaining detailed, secure and accurate records of reported online safety concerns as well as the decisions and whether or not the referrals have been made.
- Understand the purpose of record keeping.

- Monitoring online safety incidents to identify trends and any gaps in the school's provision and using this data to update the school's procedures.
- Reporting to the Local Governing Board about online safety on a termly basis.
- Working with the headteacher and Turn IT On to conduct termly light-touch reviews of this policy.

Turn IT On will be responsible for:

- Providing technical support in the development and implementation of the trust's online safety policies and procedures.
- Implementing appropriate security measures as directed by the headteachers.
- Ensuring that the trust's filtering and monitoring systems are updated as appropriate.
- Working with the DSL and headteacher to conduct termly light-touch reviews of this policy.

All staff members will be responsible for:

- Taking responsibility for the security of ICT systems and electronic data they use or have access to.
- Modelling good online behaviours.
- Maintaining a professional level of conduct in their personal use of technology.
- Having an awareness of online safety issues.
- Ensuring they are familiar with, and understand, the indicators that pupils may be unsafe online.
- Reporting concerns in line with the school's reporting procedure.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

Pupils will be responsible for:

- Adhering to the IT and Devices Acceptable Use Policy and other relevant policies.
- Seeking help from school staff if they are concerned about something they or a peer have experienced online.
- Reporting online safety incidents and concerns in line with the procedures within this policy.

Managing Online Safety

All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people, particularly with social media and the increased prevalence of children using the internet.

The DSL and school leaders have overall responsibility for their school's approach to online safety, with support from the Deputy DSL where appropriate, and will ensure that there are strong processes

in place to handle any concerns about pupils' safety online. The DSL should liaise with the police or children's social care services for support responding to harmful online sexual behaviour.

The importance of online safety is integrated across all school operations in the following ways:

- Staff and governors receive regular training
- Staff receive regular email updates regarding online safety information and any changes to online safety guidance or legislation
- Online safety is integrated into learning throughout the curriculum
- Assemblies are conducted termly on the topic of remaining safe online
- Use of Jigsaw PSHE curriculum
- Access to online safety workshops
- Use of pastoral programmes and relevant national initiatives and opportunities
- Tailored sessions based on the needs of learners

Handling Online Safety Concerns

Pupils

Any disclosures made by pupils to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Child Protection and Safeguarding Policy.

Staff will be aware that harmful online sexual behaviour can progress on a continuum, and appropriate and early intervention can prevent abusive behaviour in the future. Staff will also acknowledge that pupils displaying this type of behaviour are often victims of abuse themselves and should be suitably supported.

The victim of online harmful sexual behaviour may ask for no one to be told about the abuse, however, it is our duty to report. The DSL and other appropriate staff members will meet with the victim's parents, if appropriate, to discuss the safeguarding measures that are being put in place to support their child and how the report will progress.

Confidentiality will not be promised, and information may be still shared lawfully, for example, if the DSL decides that there is a legal basis under UK GDPR such as the public task basis whereby it is in the public interest to share the information. If the decision is made to report abuse to children's social care or the police against the victim's wishes, this must be handled extremely carefully – the reasons for sharing the information should be explained to the victim and appropriate specialised support should be offered.

Concerns regarding a pupil's online behaviour are reported to the DSL, who investigates concerns with relevant colleagues, e.g. the headteacher and Turn IT On, and manages concerns in accordance with relevant policies depending on their nature, e.g. the Behaviour Policy and Child Protection and Safeguarding Policy.

Schools will avoid unnecessarily criminalising pupils, but will contact the police, where criminal behaviour is suspected. Pupils will be provided with strong guidance if it is thought if they have acted

inadvertently as a result of ignorance or normal developmental curiosity, e.g. a pupil has taken and distributed indecent imagery of themselves. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Child Protection and Safeguarding Policy

Staff

Concerns regarding a staff member's online behaviour are reported to the headteacher, who decides on the best course of action in line with the relevant policies and HR advice. They should consult with the Chief Operations Manager (COM). If the concern is about the headteacher, it is reported to the Chief Executive Officer (CEO). Concerns will be logged on CPOMS StaffSafe. The LADO is to be consulted depending on the nature of the concern.

Where there is a concern that illegal activity has taken place, the headteacher contacts the police and the CEO.

The CEO will deal with matters in relation to headteachers and central team members. The Chair of the Trustees must be contacted if concerns are raised about the CEO.

All online safety incidents and responses are recorded by the DSL via CPOMS.

Cyberbullying

Cyberbullying can include, but is not limited to, the following:

- Threatening, intimidating or upsetting text messages.
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras.
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible.
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name.
- Unpleasant messages sent via instant messaging.
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites.
- Abuse between young people in intimate relationships online i.e. relationship abuse.
- Discriminatory bullying online i.e. homophobia, racism, misogyny/misandry.

School will be aware that certain pupils with protected characteristics can be more at risk of abuse and/or bullying online, such as LGBTQ+ pupils and pupils with SEND.

Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the KAT Anti-harassment and Bullying Policy.

Child-on-child sexual abuse and harassment

All staff will be aware of the indicators of abuse, neglect and exploitation and understand where the risk of such harms can occur online. Staff will understand that this can occur both in and outside of school, off and online, and will remain aware that pupils are less likely to report concerning online

sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

- Threatening, facilitating or encouraging sexual violence.
- Upskirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks.
- Sexualised online bullying, e.g. sexual jokes or taunts.
- Unwanted and unsolicited sexual comments and messages.
- Consensual or non-consensual sharing of sexualised imagery.
- Abuse between young people in intimate relationships online, i.e. relationship abuse.

All staff will be aware of and promote a zero-tolerance approach to sexually harassing or abusive behaviour, and any attempts to pass such behaviour off as trivial or harmless, is not acceptable behaviour and will be dealt in line with the Disciplinary Procedure Policy. Staff will be aware that allowing such behaviour would lead to a school culture that normalises abuse and leads to pupils becoming less likely to report such conduct.

Staff will be aware that creating, possessing, and distributing indecent imagery of other children, i.e. individuals under the age of 18, is a criminal offence, even where the imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves.

Schools will be aware that interactions between the victim of online harmful sexual behaviour and the alleged perpetrator(s) are likely to occur over social media following the initial report, as well as interactions with other pupils taking "sides", often leading to repeat harassment. Schools will respond to these incidents in line with the child-on-child abuse guidance in the Child Protection and Safeguarding Policy.

School leaders will respond to all concerns regarding online child-on-child sexual abuse and harassment, regardless of whether the incident took place on the school premises or using school-owned equipment. Concerns regarding online child-on-child abuse will be reported to the DSL, who will investigate the matter in line with the child-on-child abuse guidance in the Child Protection and Safeguarding Policy.

Grooming and Exploitation

Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.

Staff will be aware that grooming often takes place online and that pupils who are being groomed are commonly unlikely to report this behaviour for many reasons, e.g. the pupil may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.

Due to the fact pupils are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse. The DSL, in their annual safeguarding training, will ensure that online safety training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming are, including:

- Being secretive about how they are spending their time online.
- Having an older boyfriend or girlfriend, usually one that does not attend the school and whom their close friends have not met.
- Having money or new possessions, e.g. clothes and technological devices, that they cannot or will not explain.

Child sexual exploitation (CSE) and child criminal exploitation (CCE)

Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a pupil may be groomed online to become involved in a wider network of exploitation, e.g. the production of child pornography or forced child prostitution and sexual trafficking.

CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser, e.g. drug transporting, shoplifting and serious violence. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet.

Where staff have any concerns about pupils with relation to CSE or CCE, they will bring these concerns to the DSL without delay, who will manage the situation in line with the Child Protection and Safeguarding Policy.

Radicalisation

Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment, e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda. Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.

Staff members will be aware of the factors which can place certain pupils at increased vulnerability to radicalisation, as outlined in the Prevent Duty guidance in the Child Protection and Safeguarding Policy. Staff will be expected to exercise vigilance towards any pupils displaying indicators that they have been, or are being, radicalised.

Where staff have a concern about a pupil relating to radicalisation, they will report this to the DSL without delay, who will handle the situation in line with the Prevent Duty guidance in the Child Protection and Safeguarding Policy.

Mental Health

Staff will be aware that online activity both in and outside of school can have a substantial impact on a pupil's mental state, both positively and negatively. The relevant staff member will ensure that training is available to help ensure that staff members understand popular social media sites and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a pupil is suffering from challenges in their mental health. Concerns about the mental health of a pupil will be dealt with in line with the Mental Health and Wellbeing Policy.

Online hoaxes and harmful online challenges

For the purposes of this policy, an **“online hoax”** is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online social media platforms.

For the purposes of this policy, **“harmful online challenges”** refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media channels and daring others to do the same. Although many online challenges are harmless, an online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly as a result of partaking in the challenge itself or indirectly as a result of the distribution of the video online – the latter will usually depend on the age of the pupil and the way in which they are depicted in the video.

Where staff suspect there may be a harmful online challenge or online hoax circulating amongst pupils in the school, they will report this to the DSL/Headteacher immediately.

The DSL/Headteacher will conduct a case-by-case assessment for any harmful online content brought to their attention, establishing the scale and nature of the possible risk to pupils, and whether the risk is one that is localised to the school or the local area, or whether it extends more widely across the country. Where the harmful content is prevalent mainly in the local area, the DSL/Headteacher will consult with the police and Children's Services about whether quick local action can prevent the hoax or challenge from spreading more widely.

Prior to deciding how to respond to a harmful online challenge or hoax, the DSL and the headteacher will decide whether each proposed response is:

- In line with any advice received from a known, reliable source, e.g. the UK Safer Internet Centre, when fact-checking the risk of online challenges or hoaxes.
- Careful to avoid needlessly scaring or distressing pupils.
- Not inadvertently encouraging pupils to view the hoax or challenge where they would not have otherwise come across it, e.g. where content is explained to younger pupils but is almost exclusively being shared amongst older pupils.
- Proportional to the actual or perceived risk.

- Helpful to the pupils who are, or are perceived to be, at risk.
- Appropriate for the relevant pupils' age and developmental stage.
- Supportive.
- In line with the Child Protection and Safeguarding Policy.

Where the DSL and headteacher's assessment finds an online challenge to be putting pupils at risk of harm, they will ensure that the challenge is directly addressed to the relevant pupils, e.g. those within a particular age range that is directly affected or individual pupils at risk where appropriate.

The DSL and headteacher will only implement a school-wide approach to highlighting potential harms of a hoax or challenge when the risk of needlessly increasing pupils' exposure to the risk is considered and mitigated as far as possible.

Cyber-crime

Cyber-crime is criminal activity committed using computers and/or the internet. There are two key categories of cyber-crime:

1. **Cyber-enabled** – these crimes can be carried out offline; however, are made easier and can be conducted at higher scales and speeds online, e.g. fraud, purchasing and selling of illegal drugs, and sexual abuse and exploitation.
2. **Cyber-dependent** – these crimes can only be carried out online or by using a computer, e.g. making, supplying or obtaining malware, illegal hacking, and 'booting', which means overwhelming a network, computer or website with internet traffic to render it unavailable.

Leaders will factor their approach to online safety the risk that pupils with a particular affinity or skill in technology may become involved, whether deliberately or inadvertently, in cyber-crime. Where there are any concerns about a pupil's use of technology and their intentions with regard to using their skill and affinity towards it, the DSL will consider a referral to the Cyber Choices programme, which aims to intervene where children are at risk of committing cyber-crime and divert them to a more positive use of their skills and interests.

The DSL and headteacher will ensure that pupils are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully.

In addition, the school will implement a cyber awareness plan for pupils and staff to ensure that they understand the basics of cyber security and protecting themselves from cyber-crime.

The school will implement its cyber security strategy in line with the DfE's 'Cyber security standards for schools and colleges' and the Cyber Security Policy.

Online Safety Training for Staff

The DSL and headteacher will ensure that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation, and understanding the

expectations, roles and responsibilities relating to filtering and monitoring systems. All staff will be made aware that pupils are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life.

Online Safety and the Curriculum

Online safety is embedded throughout the curriculum; however, it is particularly addressed in the following curriculum areas:

- Relationships, Sex and Health Education (RSHE)
- PSHE
- Computing

Online safety teaching is always appropriate to pupils' ages and developmental stages.

Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using. The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

- How to evaluate what they see online.
- How to recognise techniques used for persuasion.
- Acceptable and unacceptable online behaviour.
- How to identify online risks.
- How and when to seek support.
- Knowledge and behaviours that are covered in the government's online media literacy strategy.

The online risks pupils may face online are always considered when developing the curriculum. The risks that are considered and how they are covered in the curriculum can be found in [appendix A](#) of this policy.

School leaders will develop the school's online safety curriculum. Pupils will be consulted on the online safety curriculum, where appropriate, due to their unique knowledge of the kinds of websites they and their peers frequent and the kinds of behaviours in which they engage online.

Relevant members of staff, e.g. the SENCO and designated teacher for looked after children (LAC) and previously looked after children (PLAC), will work together to ensure the curriculum is tailored so that pupils who may be more vulnerable to online harms, e.g. pupils with SEND and LAC/PLAC, receive the information and support they need.

Leaders will also endeavour to take a more personalised or contextualised approach to teaching about online safety for more susceptible children, and in response to instances of harmful online behaviour from pupils.

Class teachers will review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils.

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The headteacher and DSL will decide when it is appropriate to invite external groups into school and ensure the visitors selected are appropriate.

Before conducting a lesson or activity on online safety, the class teacher and DSL/or school leaders will consider the topic that is being covered and the potential that pupils in the class have suffered or may be suffering from online abuse or harm in this way. The DSL/or school leaders will advise the staff member on how to best support any pupil who may be especially impacted by a lesson or activity. Lessons and activities will be planned carefully so they do not draw attention to a pupil who is being or has been abused or harmed online, to avoid publicising the abuse.

During an online safety lesson or activity, the class teacher will ensure a safe environment is maintained in which pupils feel comfortable to say what they feel and ask questions and are not worried about getting into trouble or being judged.

If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will make a report in line with the Child Protection and Safeguarding Policy.

If a pupil makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member will follow the reporting procedure outlined in the Child Protection and Safeguarding Policy.

Use of Technology in the Classroom

A wide range of technology will be used during lessons, including the following:

- Laptops
- Tablets/iPads
- Cameras

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that pupils use these platforms at home, the class teacher will review and evaluate the resource. Class teachers will ensure that any internet-derived materials are used in line with copyright law.

Pupils will be supervised when using online materials during lesson time – this supervision is suitable to their age and ability.

Use of Smart Technology

While the trust recognises that the use of smart technology can have educational benefits, there are also a variety of associated risks which the trust will ensure it manages.

Pupils will be educated on the acceptable and appropriate use of technology in line with the trust's IT and Devices Acceptable Use Agreement for Pupils.

Staff will use all smart technology and personal technology in line with the trust's IT and Devices Acceptable Use Policy.

The trust recognises that pupils' unlimited and unrestricted access to the internet via mobile phone networks means that some pupils may use the internet in a way which breaches the trust's IT and Devices Acceptable Use Policy agreement for pupils.

Inappropriate use of smart technology may include:

- Using mobile and smart technology to sexually harass, bully, troll or intimidate peers.
- Sharing indecent images, both consensually and non-consensually.
- Viewing and sharing pornography and other harmful content.

Pupils will not be permitted to use smart devices or any other personal technology whilst in school.

Where there is a significant problem with the misuse of smart technology among pupils, schools will follow the school's individual Behaviour Policy.

Assemblies or workshops can be utilised where appropriate, which address any specific concerns related to the misuse of smart technology and outline the importance of using smart technology in an appropriate manner.

School Leaders will seek to ensure that it is kept up to date with the latest devices, platforms, apps, trends and related threats.

School Leaders will consider the 4Cs (content, contact, conduct and commerce) when educating pupils about the risks involved with the inappropriate use of smart technology and enforcing the appropriate disciplinary measures.

Educating Parents/Carers

Each school will work in partnership with parents/carers to ensure pupils stay safe online at school and at home. Parents will be sent a copy of the IT and Devices Acceptable Use Agreement for Pupils at the beginning of each academic year to all year groups and are expected to go through this with their child to ensure their child understands the document and the implications of not following it. This will be signed by parents/carers and pupils and returned to school annually.

Parents/carers will be made aware of the various ways in which their children may be at risk online, including, but not limited to:

- Child sexual abuse, including grooming.
- Exposure to radicalising content.
- Sharing of indecent imagery of pupils, e.g. sexting.
- Cyberbullying.
- Exposure to age-inappropriate content, e.g. pornography.
- Exposure to harmful content, e.g. content that encourages self-destructive behaviour.

Parents/carers will be informed of the ways in which they can prevent their child from accessing harmful content at home, e.g. by implementing parental controls to block age-inappropriate content.

Parental awareness regarding how they can support their children to be safe online will be raised in the following ways:

- Parents' evenings
- Workshops/ training sessions
- Newsletters
- Online resources

Internet Access

Pupils, staff and other members will only be granted access to the trust's internet network once they have read and signed the IT and Devices Acceptable Use Agreement. A record will be kept of users who have been granted internet access in the school office.

Whilst in school, working on school devices, all members of the trust community will use the trust's internet network, instead of 3G, 4G and 5G networks, as the network has appropriate filtering and monitoring to ensure individuals are using the internet appropriately.

Visitors who require internet access in school premises will be issued with a password for the school's guest Wi-Fi. A register of who has access to the guest Wi-Fi at any particular time will be kept in the school office and the visitor will sign in and out of this register.

Internet access for groups using the Keystone Training Room located in the Keystone Office at Bourne Westfield Primary Academy will be via a separate VLAN. This will allow use of personal devices with only basic internet filtering provided by Securly. Passwords will be changed regularly and frequently via a ticket to Turn IT On and will be controlled by the Governance and Operations Lead.

School staff are responsible for identifying the needs of their visitors and ensuring they have the up-to-date login details.

Filtering and Monitoring Online Activity

The Local Governing Board will ensure the school's ICT network has appropriate filters and monitoring systems in place and that it is meeting the DfE's '[Filtering and monitoring standards for schools and colleges](#)'. The Local Governing Board will check if 'over blocking' leads to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

The DSL and headteacher will ensure that specific roles and responsibilities are identified and assigned to individuals in order to manage filtering and monitoring systems and to ensure they meet the school's safeguarding needs.

The filtering and monitoring systems the school implements will be appropriate to pupils' ages, the number of pupils using the network, how often pupils access the network, and the proportionality of costs compared to the risks. Turn IT On will undertake monthly checks on the filtering and monitoring systems to ensure they are effective and appropriate and report to the trust. These results are to be included in the monthly reports issued to the trust.

Requests regarding making changes to the filtering system will be directed to the headteacher/DSL. Prior to making any changes to the filtering system, Turn IT On and the DSL/headteacher will conduct a risk assessment. Any changes made to the system will be recorded by Securly. Reports of inappropriate websites or materials will be made to the DSL/other responsible staff member immediately, who will investigate the matter and makes any necessary changes.

Deliberate breaches of the filtering system will be reported to the DSL, who will escalate the matter appropriately. If a pupil has deliberately breached the filtering system, they will be disciplined in line with the Behaviour Policy. If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Disciplinary Procedure Policy.

If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g. LADO, the Internet Watch Foundation (IWF), CEOP and/or the police.

The trust's network and school-owned devices will be appropriately monitored. All users of the network and school-owned devices will be informed about how and why they are monitored. Concerns identified through monitoring will be reported to the DSL who will manage the situation in line with the Child Protection and Safeguarding Policy.

Network Security

Technical security features, such as anti-virus software, will be kept up-to-date and managed by Turn IT On. Firewalls will be switched on at all times. Third party providers will review the firewalls regularly to ensure they are running correctly, and to carry out any required updates.

Staff and pupils will be advised not to download unapproved software or open unfamiliar email attachments and will be expected to report all malware and virus attacks to Turn IT On.

All members of staff will have their own unique usernames and private passwords to access the trust's systems. Pupils will be provided with their own unique username and passwords. Staff members and pupils will be responsible for keeping their passwords private. Passwords will have a minimum and maximum length and require a mixture of letters, numbers and symbols (appropriate to pupil age) to ensure they are as secure as possible. Passwords will expire after 365 days, after which users will be required to change them.

Users will inform Turn IT On if they forget their login details. Users will not be permitted to share their login details with others and will not be allowed to log in as another user at any time. If a user is found to be sharing their login details or otherwise mistreating the password system, the headteacher will be informed and will decide the necessary action to take.

Users will be required to lock access to devices and systems when they are not in use.

Full details of the trust's network security measures can be found in the Cyber Security Policy.

Emails

Access to and the use of emails will be managed in line with the Data Protection Policy and IT and Devices Acceptable Use Policy.

Staff will be given approved school email accounts and will only be able to use these accounts at school and when doing school-related work outside of school hours. Pupils will use their email account as their username only; pupils do not receive or send email messages. Prior to being authorised to use the email system, staff must agree to and sign the IT and Devices Acceptable Use Policy. Personal email accounts will not be permitted to be used on school devices. Any email that contains sensitive or personal information will only be sent using secure and encrypted email.

Staff members will be required to block spam and junk mail and report the matter to Turn IT On should the spam or junk emails persist. The trust's monitoring system can detect inappropriate links, malware and profanity within emails – staff are made aware of this. Chain letters, spam and all other emails from unknown sources will be deleted without being opened. Any cyber-attacks initiated through emails will be managed in line with the Cyber Response and Recovery Plan.

Generative Artificial Intelligence (AI)

All schools will take steps to prepare pupils for changing and emerging technologies, e.g. generative AI and how to use them safely and appropriately with consideration given to pupils' age at an appropriate developmental stage in their provision.

The trust will ensure its IT system includes appropriate filtering and monitoring systems to limit pupil's ability to access or create harmful or inappropriate content through generative AI.

The school will ensure that pupils are not accessing or creating harmful or inappropriate content, including through generative AI.

The school will take steps to ensure that personal and sensitive data is not entered into generative AI tools and that it is not identifiable.

Keystone Academy Trust will make use of any guidance and support that enables it to have a safe, secure and reliable foundation in place before using more powerful technology such as generative AI.

Social Networking

The use of social media by staff and pupils will be managed in line with the school's IT and Devices Acceptable Use Policies.

School Website

The headteacher will be responsible for the overall content of the school website – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements.

Use of Devices

Staff members and pupils will be issued with school-owned devices to assist with their work, where necessary. Requirements around the use of school-owned devices can be found in the IT and Devices Acceptable Use Policy (staff) and IT Acceptable Use Policy (Pupils).

Pupils will not be permitted to use smart devices or any other personal technology whilst in school.

Staff will only use personal devices during out-of-school hours, including break and lunch times. They will ensure personal devices are either switched off or set to silent mode during school hours and only make or receive calls in specific areas, e.g. the staff room. Staff will store personal devices appropriately during school hours, e.g. a lockable cupboard in the classroom.

Remote Learning

All remote learning will be delivered in line with the school's remote learning provision.

Monitoring and Review

The trust recognises that the online world is constantly changing; therefore, the DSL, Turn IT On and the headteacher will conduct termly light-touch reviews of this policy to evaluate its effectiveness.

The CEO and Chief Operations Manager will review this policy in full on an annual basis and following any online safety incidents.

Any changes made to this policy are communicated to all members of the trust community.

APPENDIX A - Online Harms and Risks – Curriculum Coverage

Subject area	Description and teaching content	Curriculum area the harm or risk is covered in
How to navigate the internet and manage information		
Age restrictions	<p>Some online activities have age restrictions because they include content which is not appropriate for children under a specific age. Teaching will include the following:</p> <ul style="list-style-type: none"> • That age verification exists and why some online platforms ask users to verify their age • Why age restrictions exist • That content that requires age verification can be damaging to under-age consumers • What the age of digital consent is (13 for most platforms) and why it is important 	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> • Health education • Computing • Jigsaw PSHE
How content can be used and shared	<p>Knowing what happens to information, comments or images that are put online. Teaching will include the following:</p> <ul style="list-style-type: none"> • What a digital footprint is, how it develops and how it can affect pupils' futures • How cookies work • How content can be shared, tagged and traced • How difficult it is to remove something once it has been shared online • What is illegal online, e.g. youth-produced sexual imagery (sexting) 	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> • Relationships education • Computing • Jigsaw PSHE
Disinformation, misinformation and hoaxes	<p>Some information shared online is accidentally or intentionally wrong, misleading or exaggerated. Teaching will include the following:</p> <ul style="list-style-type: none"> • Disinformation and why individuals or groups choose to share false information in order to deliberately deceive 	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> • Jigsaw PSHE

	<ul style="list-style-type: none"> • Misinformation and being aware that false and misleading information can be shared inadvertently • Misinformation and understanding that some genuine information can be published with the deliberate intent to harm, e.g. releasing private information or photographs • Online hoaxes, which can be deliberately and inadvertently spread for a variety of reasons • That the widespread nature of this sort of content can often appear to be a stamp of authenticity, making it important to evaluate what is seen online • How to measure and check authenticity online • The potential consequences of sharing information that may not be true 	<ul style="list-style-type: none"> • KS2 and above: Computing
Fake websites and scam emails	<p>Fake websites and scam emails are used to extort data, money, images and other things that can either be used by the scammer to harm the person targeted or sold on for financial, or other, gain. Teaching will include the following:</p> <ul style="list-style-type: none"> • How to recognise fake URLs and websites • What secure markings on websites are and how to assess the sources of emails • The risks of entering information to a website which is not secure • What pupils should do if they are harmed, targeted, or groomed as a result of interacting with a fake website or scam email • Who pupils should go to for support • The risk of 'too good to be true' online offers, advertising and fake product sales designed to persuade people to part with money for products and services that do not exist 	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> • Jigsaw PSHE • Computing
Online fraud	<p>Fraud can take place online and can have serious consequences for individuals and organisations. Teaching will include the following:</p> <ul style="list-style-type: none"> • What identity fraud, scams and phishing are • That online fraud can be highly sophisticated and that anyone can be a victim 	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> • Jigsaw PSHE • Computing

	<ul style="list-style-type: none"> • How to protect yourself and others against different types of online fraud • How to identify 'money mule' schemes and recruiters • The risk of online social engineering to facilitate authorised push payment fraud, where a victim is tricked into sending a payment to the criminal • The risk of sharing personal information that could be used by fraudsters • That children are sometimes targeted to access adults' data • What 'good' companies will and will not do when it comes to personal details • How to report fraud, phishing attempts, suspicious websites and adverts 	
Password phishing	<p>Password phishing is the process by which people try to find out individuals' passwords so they can access protected content. Teaching will include the following:</p> <ul style="list-style-type: none"> • Why passwords are important, how to keep them safe and that others might try to get people to reveal them • How to recognise phishing scams • The importance of online security to protect against viruses that are designed to gain access to password information • What to do when a password is compromised or thought to be compromised 	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> • Jigsaw PSHE • Computing
Personal data	<p>Online platforms and search engines gather personal data – this is often referred to as 'harvesting' or 'farming'. Teaching will include the following:</p> <ul style="list-style-type: none"> • How cookies work • How data is farmed from sources which look neutral • How and why personal data is shared by online companies • How pupils can protect themselves and that acting quickly is essential when something happens • The rights children have with regards to their data • How to limit the data companies can gather 	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> • Jigsaw PSHE • Computing

Persuasive design	<p>Many devices, apps and games are designed to keep users online for longer than they might have planned or desired. Teaching will include the following:</p> <ul style="list-style-type: none"> • That the majority of games and platforms are designed to make money, and that their primary driver is to encourage people to stay online for as long as possible to encourage them to spend money or generate advertising revenue • How notifications are used to pull users back online 	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> • Jigsaw PSHE • Computing
Privacy settings	<p>Almost all devices, websites, apps and other online services come with privacy settings that can be used to control what is shared. Teaching will include the following:</p> <ul style="list-style-type: none"> • How to find information about privacy settings on various sites, apps, devices and platforms • That privacy settings have limitations 	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> • Jigsaw PSHE • Computing
Targeting of online content	<p>Much of the information seen online is a result of some form of targeting. Teaching will include the following:</p> <ul style="list-style-type: none"> • How adverts seen at the top of online searches and social media have often come from companies paying to be on there and different people will see different adverts • How the targeting is done • The concept of clickbait and how companies can use it to draw people to their sites and services 	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> • Jigsaw PSHE • Computing
How to stay safe online		
Online abuse	<p>Some online behaviours are abusive. They are negative in nature, potentially harmful and, in some cases, can be illegal. Teaching will include the following:</p> <ul style="list-style-type: none"> • The types of online abuse, including sexual harassment, bullying, trolling and intimidation • When online abuse can become illegal • How to respond to online abuse and how to access support • How to respond when the abuse is anonymous • The potential implications of online abuse 	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> • Jigsaw PHSE • Computing

	<ul style="list-style-type: none"> What acceptable and unacceptable online behaviours look like 	
Radicalisation	<p>Pupils are at risk of accessing inappropriate and harmful extremist content online, including terrorist material. Extremist and terrorist groups use social media to identify and target vulnerable individuals. Teaching will include the following:</p> <ul style="list-style-type: none"> How to recognise extremist behaviour and content online Which actions could be identified as criminal activity Techniques used for persuasion How to access support from trusted individuals and organisations 	All areas of the curriculum
Challenges	<p>Online challenges acquire mass followings and encourage others to take part in what they suggest. Teaching will include the following:</p> <ul style="list-style-type: none"> What an online challenge is and that, while some will be fun and harmless, others may be dangerous and even illegal How to assess if the challenge is safe or potentially harmful, including considering who has generated the challenge and why That it is okay to say no and to not take part in a challenge How and where to go for help The importance of telling an adult about challenges which include threats or secrecy, such as 'chain letter' style challenges 	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> Jigsaw PSHE
Content which incites violence	<p>Knowing that violence can be incited online and escalate very quickly into offline violence. Teaching will include the following:</p> <ul style="list-style-type: none"> That online content (sometimes gang related) can glamorise the possession of weapons and drugs That to intentionally encourage or assist in an offence is also a criminal offence How and where to get help if they are worried about involvement in violence 	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> Jigsaw PSHE

Fake profiles	<p>Not everyone online is who they say they are. Teaching will include the following:</p> <ul style="list-style-type: none"> • That, in some cases, profiles may be people posing as someone they are not or may be 'bots' • How to look out for fake profiles 	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> • Jigsaw PSHE • Computing
Grooming	<p>Knowing about the different types of grooming and motivations for it, e.g. radicalisation, child sexual abuse and exploitation, gangs and financial exploitation. Teaching will include the following:</p> <ul style="list-style-type: none"> • Boundaries in friendships with peers, in families, and with others • Key indicators of grooming behaviour • The importance of disengaging from contact with suspected grooming and telling a trusted adult • How and where to report grooming both in school and to the police <p>At all stages, it is important to balance teaching pupils about making sensible decisions to stay safe whilst being clear it is never the fault of the child who is abused and why victim blaming is always wrong.</p>	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> • Jigsaw PSHE
Unsafe communication	<p>Knowing different strategies for staying safe when communicating with others, especially people they do not know or have not met. Teaching will include the following:</p> <ul style="list-style-type: none"> • That communicating safely online and protecting your privacy and data is important, regardless of who you are communicating with • How to identify indicators of risk and unsafe communications • The risks associated with giving out addresses, phone numbers or email addresses to people pupils do not know, or arranging to meet someone they have not met before • What online consent is and how to develop strategies to confidently say no to both friends and strangers online 	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> • Jigsaw PSHE • Computing

Wellbeing		
Impact on quality of life, physical and mental health and relationships	<p>Knowing how to identify when online behaviours stop being fun and begin to create anxiety, including that there needs to be a balance between time spent online and offline. Teaching will include the following:</p> <ul style="list-style-type: none"> • How to evaluate critically what pupils are doing online, why they are doing it and for how long (screen time) • How to consider quality vs. quantity of online activity • The need for pupils to consider if they are actually enjoying being online or just doing it out of habit, due to peer pressure or due to the fear of missing out • That time spent online gives users less time to do other activities, which can lead some users to become physically inactive • The impact that excessive social media usage can have on levels of anxiety, depression and other mental health issues • That isolation and loneliness can affect pupils and that it is very important for them to discuss their feelings with an adult and seek support • Where to get help 	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> • Jigsaw PSHE • PE • Pastoral support where required
Online vs. offline behaviours	<p>People can often behave differently online to how they would act face to face. Teaching will include the following:</p> <ul style="list-style-type: none"> • How and why people can often portray an exaggerated picture of their lives (especially online) and how that can lead to pressure • How and why people are unkind or hurtful online when they would not necessarily be unkind to someone face to face 	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> • Relationships education
Suicide, self-harm and eating disorders	<p>Pupils may raise topics including eating disorders, self-harm and suicide. Teachers must be aware of the risks of encouraging or making these seem a more viable option for pupils and should take care to avoid giving instructions or methods and avoid using language, videos and images.</p>	