KING EDWARD VI
SCHOOL LICHFIELD

Online Safety Policy

2026

Original Version:	Ratified on 12/10/2023, now superseded
To be reviewed by:	Assistant Headteacher Community
Governors Review: Summary of Changes: Ratified by: Date:	 Major revision, informed by The Key Student & Staff Welfare Committee 11/06/2026
Version:	FINAL
Dissemination: Teams policy folder KES website Other	 √ √ √ KES All Staff Team
Next Review:	Summer 2028

Contents

Aims 3
Legislation and guidance 3
Roles and responsibilities 4
Educating students about online safety 7
Educating parents/carers about online safety 7
Cyber-bullying 10
Acceptable use of the internet in school 12
Students using mobile devices in school 13
Staff using work devices outside school 13
How the school will respond to issues of misuse 13
Training 14
Monitoring arrangements 15
Links with other policies 15
Appendix 1: Acceptable use agreement (students and parents/carers) 16
Appendix 2: Acceptable use agreement (staff, governors, volunteers and visitors) 18

1. Aims

King Edward VI School aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, misinformation, disinformation (including fake news,) conspiracy theories, racism, misogyny, self-harm, suicide, anti-Semitism, 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; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

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

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on students electronic devices where they believe there is a 'good reason' to do so.

3. Roles and responsibilities

3.1 The Governing Body

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will ensure all staff undergo online safety training as part of child protection and safeguarding training, and that staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and the termly meeting between the DSL and link Safeguarding governor will include online safety logs monitoring.

The governing board will make sure that the school teaches students how to keep themselves and others safe, including online.

The governing board will make sure that the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE's filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- ✔ Identifying and assigning roles and responsibilities to manage filtering and monitoring systems
- ✔ Reviewing filtering and monitoring provisions at least annually
- ✔ Blocking harmful and inappropriate content without unreasonably impacting teaching and learning
- ✔ Having effective monitoring strategies in place that meet the school's safeguarding needs

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some students

with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The Headteacher

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

3.3 The Designated Safeguarding Lead

Details of the school's DSL and Deputy DSLs are set out in our 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, ICT manager and other staff, as necessary, to address any online safety issues or incident
- 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
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Responding to safeguarding concerns identified by filtering and monitoring
- 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
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board

This list is not intended to be exhaustive.

3.4 The Network manager

The Network manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated at least annually to assess effectiveness and ensure students are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are reported so they can be dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet and ensuring that students follow the school's terms on acceptable use – appendix 2
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes and being aware of how to report incidents. This should be done in line with our school's behaviour and safeguarding policy.
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

Contractors and agency staff do not access the network. If this was necessary for any reason then we would supply this policy.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet – appendix 1
- Ensure they are safe when using the internet - be aware of their use of social media and online activity.

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

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International
- Our website page for online safety is regularly updated Online Safety - King Edward VI

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use – appendix 2

4. Educating students about online safety

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

In **Key Stage 3**, students will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns
- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the **end of secondary school**, students will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- Online risks, including the importance of being cautious about sharing personal information online and of using privacy and location settings appropriately to protect information online. Students should also understand the difference between public and private online spaces and related safety issues
- The characteristics of social media, including that some social media accounts are fake, and / or may post things which aren't real / have been created with AI.

- That social media users may say things in more extreme ways than they might in face-to-face situations, and that some users present highly exaggerated or idealised profiles of themselves online
- Not to provide material to others that they would not want to be distributed further and not to pass on personal material which is sent to them. Students should understand that any material provided online might be circulated, and that once this has happened there is no way of controlling where it ends up. Students should understand the serious risks of sending material to others, including the law concerning the sharing of images
- That keeping or forwarding indecent or sexual images of someone under 18 is a crime, even if the photo is of themselves or of someone who has consented, and even if the image was created by the child and/or using AI-generated imagery. Students should understand the potentially serious consequences of acquiring or generating indecent or sexual images of someone under 18, including the potential for criminal charges and severe penalties including imprisonment. Students should know how to seek support and should understand that they will not be in trouble for asking for help, either at school or with the police, if an image of themselves has been shared. Students should also understand that sharing indecent images of people over 18 without consent is a crime
- What to do and how to report when they are concerned about material that has been circulated, including personal information, images or videos, and how to manage issues online About the prevalence of deepfakes including videos and photos, how deepfakes can be used maliciously as well as for entertainment, the harms that can be caused by deepfakes and how to identify them
- The impact of viewing harmful content
- That the internet contains inappropriate and upsetting content, some of which is illegal, including unacceptable content that encourages misogyny, violence or use of weapons. Students should be taught where to go for advice and support about something they have seen online. Students should understand that online content can present a distorted picture of the world and normalise or glamorise behaviours which are unhealthy and wrong
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- That social media can lead to escalations in conflicts, how to avoid these escalations and where to go for help and advice. How to identify when technology and social media is used as part of bullying, harassment, stalking, coercive and controlling behaviour, and other forms of abusive and/or illegal behaviour and how to seek support about concerns
- That pornography, and other online content, often presents a distorted picture of people and their sexual behaviours and can negatively affect how people behave towards sexual partners. This can affect students who see pornographic content accidentally as well as those who see it deliberately. Pornography can

also portray misogynistic behaviours and attitudes which can negatively influence those who see it

- That websites may share personal data about their users, and information collected on their internet use, for commercial purposes (e.g. to enable targeted advertising)
- That criminals can operate online scams, for example using fake websites or emails to extort money or valuable personal information. This information can be used to the detriment of the person or wider society. About risks of sextortion, how to identify online scams relating to sex, and how to seek support if they have been scammed or involved in sextortion
- That AI chatbots are an example of how AI is rapidly developing, and that these can pose risks by creating fake intimacy or offering harmful advice. It is important to be able to critically think about new types of technology as they appear online and how they might pose a risk
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

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

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

4.1 Students will be taught practical cyber security skills

The following items come from the DfE's Meeting digital and technology standards in schools and colleges - Cyber security: core standard - Guidance - GOV.UK

All students will receive age-appropriate training on safe internet use, including:

- 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

Students will also receive age-appropriate education on safeguarding issues such as cyberbullying and the risks of online radicalisation.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters, newsletters or other communications home, and in information via our website. Parents and carers of Year 7 & 8

students have an opportunity to attend an online safety information presentation. This policy will also be shared with parents.

Our safeguarding newsletter contains online safety updates, including the systems we use to filter and monitor online. We encourage parents and carers to monitor their child's electronic devices and Social Media accounts.

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

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

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Form tutors will discuss cyber-bullying with their tutor groups as part of PSHE lessons and tutor time.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support students, as part of safeguarding training.

The school also provides information (via our website and newsletters) on online safety and cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected. Parents/carers and students are encouraged to report any bullying concerns either by contacting the school office or using the designated email address which is monitored each working day by a member of the Safeguarding Team: antibullying@keslichfield.org.uk

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among students, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

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

- Poses a risk to staff or students, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other students and staff. If the search is not urgent, they will seek advice from the headteacher/DSL or member of the SLT.
- Explain to the student why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the students co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

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

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL / headteacher / other member of the senior leadership team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The student and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of students 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
- Our behaviour policy / searches and confiscation policy

Any complaints about searching for or deleting inappropriate images or files on students electronic devices will be dealt with through the school complaints procedure.

6.4 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, students and parents/carers may be familiar with generative chatbots such as ChatGPT and Co-Pilot.

King Edward VI School recognises that AI has many uses to help students 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.

King Edward VI School will treat any use of AI to bully students in line with our anti-bullying/behaviour policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used.

7. Acceptable use of the internet in school

All students, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-2). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

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

More information is set out in the acceptable use agreements in appendices 1 and 2.

8. Students using mobile devices in school

Students may bring mobile devices into school, but students in Years 7-11 are not permitted to use them during the school day. Phones must be switched off and in school bags. This includes before and after school clubs or any other activities organised by the school, unless explicitly directed by staff.

Any use of mobile devices in school by students must be in line with the acceptable use agreement (see appendices 1 and 2).

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

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date – always install the latest updates
- Staff members must not use the device in any way which would violate the school's terms of acceptable use
- Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the ICT support team.

10. How the school will respond to issues of misuse

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

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

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

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse

Children can abuse their peers online through:

- Abusive, harassing, and misogynistic messages
- Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
- Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to ensure students can recognise dangers and risks in online activity and can weigh the risks up
- develop the ability to influence students to make the healthiest long-term choices and keep them safe from harm in the short term

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.

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

Volunteers will receive appropriate training and updates, if applicable.

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

12. Monitoring arrangements

The DSL, deputies and member of our Student Support team with responsibility for championing online safety, log safeguarding issues related to online safety using our Safeguarding recording software – 'My Concern.' Behavioural concerns will be logged via GO4Schools.

All desktop computers in school use a filtering system provided by RM, called Safetynet. In addition to this school devices utilise monitoring software called Securus. This is monitored regularly by our DSL and/or member of our Student Support team who champions online safety.

This policy will be reviewed every two years by the Assistant Headteacher. At every review, the policy will be shared with the governing board. The review will be supported by an annual risk assessment that considers and reflects the risks students face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with other policies

This online safety policy is linked to our:

- Safeguarding and Child Protection Policy
- Behaviour policy
- Antibullying
- Data protection policy
- Complaints policy

All the above policies can be found on our website King Edward VI School policies

KING EDWARD VI
SCHOOL LICHFIELD

Appendix 1 - King Edward VI School
ICT Acceptable use agreement (students and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STUDENTS AND PARENTS/CARERS	
Name of student:	

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 member of staff is present, or with the permission of a member of staff
- Keep my username 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'm finished working on it

I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless a member of staff 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 member of staff
- Use any inappropriate language when communicating online, including in emails
- 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:

- It will remain out of sight, not used, seen or heard during the course of the school day or during school arranged activities. (For students in years 7-11). Sixth form students are permitted to use mobiles whilst working independently in the common room.

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 (student):	**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 students using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STUDENTS AND PARENTS/CARERS	
Signed (parent/carer):	Date:

Appendix 2 - King Edward VI School

ICT acceptable use agreement (staff, governors, volunteers and visitors)

KING EDWARD VI
SCHOOL LICHFIELD

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 students without checking with school staff first • Share confidential information about the school, its students 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 student 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 students in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**