King Edward VI Grammar School

Digital Devices and Online Safety Policy

Head Teacher:	Mr James Lascelles
Digital Schools Lead:	Miss Adele Teasel
Designated Safeguarding Lead:	Mrs Laura Reeve
Chair of Trustees:	Mr Robert Maltman

Contents

1. Intent and Aims

KEVIGS understands that digital literacy, digital skills, access to online sources and tools is an important aspect of raising educational standards, promoting achievement, and preparing our students for life beyond school. To be able to live, learn and work successfully in our technology-rich society, students must be able to utilize technology effectively and appropriately, therefore embedding the use of technology in learning allows our young people to begin to make informed decisions while online and using technology in their day-to-day lives.

Our school aims to:

- Set expectations for the safe and responsible use of digital technologies for learning, administration, and communication across staff, students, parents, volunteers and trustees
- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and trustees
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

This Digital Device and Online Safety Policy applies to all members of the King Edward VI Grammar School community (including staff, students, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems and personal devices both on and off the school premises.

This policy will be reviewed every year by the senior leadership team in conjunction with the online safety group. At every review, the policy will be shared with the Board of Trustees.

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 pupils' electronic devices where they believe there is a 'good reason' to do so.

3. Roles and responsibilities

3.1 The Board of Trustees

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

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

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

The Every Child Matters (ECM) Sub-Committee Group will receive regular information about online safety incidents and monitoring reports. The Safeguarding Governor's role also includes the role of the Online Safety Governor. The board of trustees will ensure children are taught how to keep themselves and others safe, including keeping safe online. The board of trustees will also support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.

The board of trustees must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those standards, which include:

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

All trustees will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The Headteacher and Senior Leaders

- The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety may be delegated to the Online Safety Lead – who is the Designated Safeguarding Lead.
- The headteacher and (at least) another member of the senior leadership team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

- The headteacher/senior leaders are responsible for ensuring that the Online Safety Lead, technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
- The headteacher/senior leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.

3.3 The Designated Safeguarding lead (DSL)

Details of the school's designated safeguarding lead (DSL) and deputy/deputies 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 and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy and the child protection policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher, senior leaders and governing board
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

3.4 The IT Support Team

The IT Support Team is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's IT 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 IT systems on a fortnightly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

- Ensuring that any online safety or misuse of ICT incidents involving students are logged on Safeguard My School and dealt with appropriately in line with this policy and that any concerns over staff conduct is shared with the Headmaster immediately.
- They keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant

This list is not intended to be exhaustive.

3.5 Curriculum Leaders

Curriculum Leads will work with the DSL and Deputy Head academic to develop a planned and coordinated online safety education programme. This will be provided through:

- RSHE Curriculum lessons
- Mapped cross-curricular opportunities.
- assemblies and pastoral programmes
- through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

3.6 All Staff and Visitors

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Read, understood, signed and adhering to the terms of acceptable use of the school's ICT systems and the internet (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)

- Taking necessary precautions to uphold the security of online platforms and safeguarding of school systems. This includes setting secure passwords and updating them regularly, using 2 Factor Authentication when necessary and not sharing log-in details with others.
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing using Safeguard My School
- Following the correct procedures by requesting via the blocked message and/or emailing IT Support if they need to bypass the filtering and monitoring systems for educational purposes.
- Working with the DSL to ensure that any online safety incidents are logged on Safeguard My School and dealt with appropriately in line with this and the behaviour policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.
- have a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc and respond appropriately to all reports and concerns both online and offline, and maintaining an attitude of 'it could happen here'
- they supervise and monitor the use of digital technologies, digital devices, cameras, etc., in lessons and other school activities and implement current policies regarding these devices.
- in lessons where internet use is pre-planned learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches through the safeguarding procedures.
- all digital communications with learners and parents/carers should be on a professional level and carried out using official school systems.

- they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.

This list is not intended to be exhaustive.

3.7 Students

- are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement (Appendix 1) and this Digital and Online Safety Policy
- should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- are responsible for identifying and reporting abuse and misuse or access to inappropriate materials to an appropriate adult or by using the Whisper App.
- should know what to do if they or someone they know feels vulnerable when using online technology
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

3.8 Parents and Carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the online services and devices in an appropriate way.

The school will take every opportunity to help parents and carers understand these issues through:

- publishing the school Online Safety Policy on the school website
- providing them with a copy of the student acceptable use agreement
- publish information about appropriate use of social media relating to posts concerning the school
- seeking their permissions concerning digital images, via the parent/carer acceptable use agreement
- parents'/carers' evenings, newsletters, website, social media and information about national/local online safety campaigns and literature.

Parents/carers are expected to:

- ensure all personal devices have the appropriate parental controls applied and regularly monitor their child's usage of these devices.
- discuss with their child the appropriate and safe use of their devices, including gaming and social media platforms, ensuring age restrictions are followed.
- ensure there is a balance between educational screen-time and personal screen-time to promote positive mental and physical health. Consider using the 'Digital 5 A Day principles'.
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's IT systems and internet (Appendix 1)
- reinforcing the online safety messages provided to learners in school.
- Ensure their child's device is learning ready; meeting the suggested minimum requirements for an appropriate device, is fully charged every day and has the required applications on it.
- notify a member of staff of any concerns or queries regarding this policy.

By enrolling their child in the school, all parents are agreeing to this Digital Devices and Online Safety Policy and will support the school in ensuring their child follows the student acceptable user agreement.
Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International

See also the Policies area of the school website.

3.9 Visitors and members of the community

Visitors and community users who access the school systems/website/learning platforms will be expected to read and sign the Acceptable Use Agreement for Staff and Visitors before being provided with access to the school systems. (Appendix 2)

4. Acceptable use of Learning Devices

4.1 Student use of devices

KEVIGS defines a Learning Device as a device that meets the minimum specifications that aid and enhance learning. These include tablet devices with an 8 inch or larger touch screen, with keyboard and stylus compatibility. This is due to the need for students to annotate and interact with digital materials.

Pupils may bring mobile devices and earphones into school, but are not permitted to use them during:

- Lessons – mobiles must be on silent (not vibrate) and placed face-down, at the top right-hand corner of their desk.
- Tutor group time
- Enrichment
- While walking to or between lessons inside school buildings.

Use of mobile phones during any of the learning times above should only be used as a last resort when the students 'learning device' is not available [authorized reasons] and only when instructed by a teacher/activity lead to do so. Teachers may require students to watch/listen to sources with audio, earphones can be used during these permitted activities.

Learning Devices will be used for:

- Working in Microsoft Teams to access learning resources, assignments and communicate between staff and students, the Assignments tab will be used to set homework assignments and monitor students' progress.
- File storage and sharing using OneDrive, SharePoint and MS Teams for the purpose of collaboration.
- OneNote – students will centralise their notes and ongoing work using OneNote
- E-Book readers such as Boost and Kerboodle to access course textbooks.
- Subscription platforms such as GCSEPod, Unifrog to support and consolidate learning.
- Access video and audio recordings to support learning (only in accordance with the Acceptable user contract)
- Subject specific applications such as, but not limited to GIS in Geography, coding software in Computer Science, and editing software in Media & Photography.
- Interactive learning applications such as Quizlet, ChatGPT, Canva, MS Forms, Microsoft Flip and may more that support learning across all subjects and key stages.

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's IT systems and the internet (Appendix 1 and Appendix 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 should be for educational purposes or for the purpose of fulfilling the duties of an individual's role.

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

We will apply the KEVIGS filtering to block harmful and/or inappropriate content being accessed while on the school site.

We monitor MS Teams using SENSO.

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

4.2. Staff using work devices outside school

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

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device.
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in appendix 2.

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 itsupport@kevigs.lincs.sch.uk .

5. Protecting Students and Staff from Online Abuse

The 4 key categories of risk

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

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism.
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

Children and young people may experience several types of abuse online:

- bullying/cyberbullying
- emotional abuse (this includes emotional blackmail, for example pressuring children and young people to comply with sexual requests via technology)
- Consensual and non-consensual sharing of nudes and semi-nude images and or videos (also known as sexting or youth produced sexual imagery) including pressure or coercion to create sexual images
- sexual abuse
- sexual exploitation.
- Radicalisation

Please see the school's annually updated Child Protection and Safeguarding Policy for further details on the safeguarding aspects of online safety.

Before using devices in school and for school related purposes, students and staff must read and agree to the Acceptable Use Agreement via the Microsoft Forms:

Student Acceptable User Agreement

Staff & Visitor Acceptable User Agreement:

5.1 Educating pupils about online safety

- Pupils will be taught about online safety as part of the curriculum and will follow national guidance e.g. Education for a Connected Work Framework by UKCIS/DCMS.
- We will incorporate relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week
- in lessons where internet use is pre-planned, it is best practice that learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- where learners are allowed to freely search the internet, staff should be vigilant in supervising the learners and monitoring the content of the websites the young people visit
- it is accepted that from time to time, for good educational reasons, students may need to research topics, (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff should be able to request the temporary removal of those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need
- the online safety education programme should be relevant and up to date to ensure the quality of learning and outcomes.

In **Key Stage 3**, pupils 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

Pupils in **Key Stage 4** will be taught:

- 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**, pupils will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence that carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- 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)

Digital competency (digital literacy and digital skills) and the safe use of social media and the internet will be planned and effectively threaded through the appropriate digital pillars in other curriculum areas e.g. PHSE; SRE; Literacy and be covered in other subjects where relevant.

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

5.2 Educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website or SIMS In Touch messages. This policy will also be shared with parents/carers.

Online safety will also be covered during parents' evenings such as Yr 7 open evening, and other Online Webinar events throughout the academic year.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents/carers have any queries or concerns in relation to online safety, they should notify a member of staff

5.3 Educating Staff & Trustees

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

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

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

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, harassing, and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

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

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

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

Volunteers will receive appropriate training and updates, if applicable.

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

5.4 Filtering

- the school filtering policies are agreed by senior leaders and technical staff and are regularly reviewed and updated in response to changes in technology and patterns of online safety incidents/behaviours
- the school manages access to content across its systems for all users. The filtering provided meets the standards defined in the UK Safer Internet Centre Appropriate filtering
- illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated
- access to online content and services is managed for all users and the school has differentiated user-level filtering (allowing different filtering levels for different abilities/ages/stages and different groups of users: staff/learners, etc.)
- there is a clear process in place to deal with requests for filtering changes
- there are established and effective routes for users to report inappropriate content
- filtering logs are regularly reviewed and alert the school to breaches of the filtering policy, which are then acted upon.

5.5 Monitoring

The school has monitoring systems in place to protect the school, systems and users:

- The school monitors network use across all its connected devices and services
- An appropriate monitoring strategy for all users has been agreed and users are aware that the network is monitored. There is a staff lead responsible for managing the monitoring strategy and processes.
- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention. Management of serious safeguarding alerts is consistent with safeguarding policy and practice
- Technical monitoring systems are up to date and managed and logs/alerts are regularly reviewed and acted upon.

The school follows the new DfE Monitoring Standards and the UK Safer Internet Centre Appropriate Monitoring guidance and protects users and school systems through the use of the appropriate blend of strategies strategy informed by the school's risk assessment. These may include:

- physical monitoring (adult supervision in the classroom)
- internet use is logged, regularly monitored and reviewed
- filtering logs are regularly analysed and breaches are reported to senior leaders
- pro-active alerts inform the school of breaches to the filtering policy, allowing effective intervention.
- where possible, school technical staff regularly monitor and record the activity of users on the school technical systems
- use of a third-party assisted monitoring service to review monitoring logs and report issues to school monitoring lead(s)

5.6 Cyber-bullying

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power.

Preventing and addressing cyber-bullying

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

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

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

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

The school gives information on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected.

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

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

5.7 How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet this is taken seriously and dealt with according to our behaviour policy and/or our child protection policy, as deemed most appropriate. 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 that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Examining electronic devices

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

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

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

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from a member of the senior leadership team/Headmaster.
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

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

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

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

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL / 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 pupil and/or the parent/carer refuses to delete the material themselves

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

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

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy: searches and confiscation section

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

6 . Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff code of conduct and HR handbook
- Data protection policy and privacy notices
- Complaints procedure

"Encouraging Excellence, Nurturing Talent"
King Edward VI Grammar School

Appendix 1: Student Acceptable Use Agreement

These rules have been written to help keep everyone safe and happy when they are online or using technology. Sometimes things go wrong and people get upset, but these rules help us avoid it where we can.

School systems and users are protected and monitored by security and filtering services to provide safe access to digital technologies. This means anything you do on a school device or using school networks/platforms/internet (including from home when home learning) may be viewed by one of the staff members who are here to keep you safe.

But it's not about systems and devices – it's about behaviour. So the same rules apply when you are at school as when you are home learning or just having fun with friends. All of the points in the this agreement below can be summarised as follows:

"Treat yourself and others with respect at all times; treat people in the same way when you are online or on a device as you would face to face."

I will read and follow the rules in the acceptable use agreement policy.

When I use devices (including mobile phones) at school I will:

- Always use the school's IT systems and the internet responsibly and for educational purposes only
- Only use them when instructed to by my teacher. When not in use for educational purposes my device(s) must be on silent (not vibrate) to prevent any disruption to learning.
- Immediately comply with any teachers'/activity leaders/school staff's request to put away/shutdown or close the screen on my device.
- Treat myself and others with respect at all times, treating others the way I would like to be treated and speaking to people as I would face to face.
- Always protect my reputation and that of the school, staff, students and others.
- Only use apps, sites and games I am old enough for. I know most social media are 13+ and games can have higher age ratings. I know 18-rated games are not just more difficult but bad.
- Keep my usernames and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Always log off or shut down a computer when I've finished working on it and ensure my personal device is not left on school premises out of school hours.
- Take steps to be academically honest and not submit plagiarised work as my own by using a recognised referencing format. This includes the use of AI such as ChatGTP.
- Tell an adult teacher immediately if I find any material which might upset, distress or harm me or others and where possible report it on the app, site or game
- If I see, watch, read, hear or receive anything I am unhappy with or I receive a message that makes me feel uncomfortable, e.g. bullying, sexual, violent or extremist/hateful content, I will not respond to it but I will talk to a trusted adult about it or report it on the Whisper App.
- I know I can also report unwanted harassment or abuse from the school community and get help at help@nspcc.org.uk or by calling 0800 136 663, as well as getting in touch with Childline, The Mix, or The Samaritans.

- Take full responsibility for my device(s). I understand that KEVIGS is not responsible for my device(s) in any way.
- Ensure appropriate internet filters are in place, I understand that I can only use my device (including mobile phones) on the KEVIGS Wi-fi and will not bypass the schools network filtering and restrictions using 3G/4G/5G networks.
- I understand that I must take all reasonable steps to avoid bringing devices onto the KEVIGS premises that might infect the network with viruses, worms or any other programme designed to damage, alter, destroy or provide access to unauthorized data or information.
- I accept that KEVIGS has the right to examine any device that is suspected of containing material that contravenes the school rules or is the source of an attack or virus infection.

I will not:

- Post, look at, up/download or share material that could be offensive, misleading, harmful or illegal. If I come across any, I will report it immediately.
- Access social networking sites, chat rooms and gaming sites during lessons unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments or follow any links in emails from an unknown sender or if it looks strange to me; I will double check with the person it is from (in a new message, not by clicking reply) or I will check with a teacher
- Use technology to bully, impersonate, harass, threaten, make fun of or upset anyone, at school or outside. I will stand up for my friends and not be a bystander.
- Post picture or personal information about students without their permission
- Post or share information or content that can negatively affect the reputation of KEVIGS or the KEVIGS community
- Use any inappropriate language when communicating online, including in emails and MS Teams Chat and all social media platforms
- Use the MS Teams Chat or other direct messaging platforms to communicate with my peers during lessons unless it is expressly allowed as part of a learning activity
- Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate
- Take secret photos, videos or recordings of teachers or students, including when learning remotely.
- Log in to the school's network using someone else's details
- Use my device(s) during tests or assessments of any kind unless otherwise specifically directed to by the teacher. As per the JCQ regulations, any smart devices or phones found on the students' person could lead to disqualification from that and all future examinations.
- Download copyright-protected material (text, music, video etc.).
- Arrange early departure from school with a parent/carer for appointments or medical emergencies; this must be arranged via our Student Reception. I should report to the medical room immediately if I am unwell or require urgent medical attention.
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision
- Use anyone else's device without their permission.

I understand that for security and safeguarding reasons the school:

- **has website filtering in place and will monitor online activity on all devices connected to the school Wi-fi.**
- **When using Microsoft Teams, including public and private chat functions will be monitored at all times when using a @kevigs.lincs.sch.uk account for identifying inappropriate messages and images.**

By completing this MS Form, confirm I have read, understood and agree to the rules included in the 'KEVIGS Acceptable Use Agreement'.
I agree to follow these guidelines when:
• I use the school's systems and devices (both in and out of school)

• I use my own devices in the school (when allowed) e.g. learning devices and mobile phones.
• I use my own equipment out of the school in a way that is related to me being a member of this school e.g. communicating with other members of the school, through school email and MS Teams and on public forums such as Social Media platforms.

"Encouraging Excellence, Nurturing Talent"
King Edward VI Grammar School

Appendix 2: Acceptable use agreement (staff, governors, volunteers and visitors)

When using the school's ICT systems and accessing the internet in school, or outside school on a device, 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 with staff, students, parents and trustees, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network without permission from the IT support manager.
- Share my password with others or log in to the school's network using someone else's details
- Take photographs of pupils without checking the 'Photographic consent status on SIMS first and will only use them for professional purposes, compatible with my professional role.
- I will not store photos of pupils on my phone beyond their intended use, eg once posted on the schools blog or social media pages etc.
- Share confidential information about the school, its pupils or staff, or other members of the community
- Share my own personal details, such as mobile phone number, personal email address, personal Twitter account, or any other social media link, to pupils.
- 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

When using the school's ICT systems and accessing the internet in school, or outside school on a device, 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, deemed appropriate by the Head or Governing body.
- Respect copyright and intellectual property rights.
- 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.
- Ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off site must be encrypted, e.g. on a password secured laptop or memory stick
- Only use my personal mobile/iPad/tablet only for approved educational activities during lesson times and/or the working school day: use during non-contact times or rest breaks is permitted.
- Support the school approach to online safety and not upload or add any images, video, sounds or text linked to or associated with the school or its community.

- Ensure that my online activity, both in school and outside school, will not bring the school, my professional reputation, or that of others, into disrepute.
- Let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.
- Support and promote the school's policies and help pupils to be safe and responsible in their use of ICT and related technologies

I understand that for security and safeguarding reasons:

- **has website filtering in place and will monitor online activity on all devices connected to the school Wi-fi.**
- **all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Head.**
- **I Understand the school reserves the right to monitor personal use and to intervene where this is excessive, interfering with the effective performance of your duties, or deemed unprofessional.**
- **I understand this forms part of the terms and conditions set out in my contract of employment.**

By completing this MS Form, confirm I have read, understood and agree to the rules included in the 'KEVIGS Acceptable Use Agreement'.
I agree to follow these guidelines when:
• I use the school's systems and devices (both in and out of school)
• I use my own devices in the school (when allowed) e.g. learning devices and mobile phones.
• I use my own equipment out of the school in a way that is related to me being a member of this school e.g. communicating with other members of the school, through school email and MS Teams and on public forums such as Social Media platforms.

Additional Notes

Monitoring of ICT access and usage ICT authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, emails, instant messaging, internet/intranet use and any other electronic communications (data, voice, video or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain school business related information; to confirm or investigate compliance with school policies, standards and procedures; to ensure the effective operation of school ICT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime.

Breaches

A breach or suspected breach of policy by a school employee, contractor or pupil may result in the temporary or permanent withdrawal of school ICT hardware, software or services from the offending individual.

For staff any policy breach is grounds for disciplinary action in accordance with the school Disciplinary Procedure or, for Support Staff, in their Probationary Period as stated.

Policy breaches may also lead to criminal or civil proceedings.

The Information Commissioner's powers to issue monetary penalties came into force on 6 April 2010, allowing the Information Commissioner's office to serve notices requiring organisations to pay up to £500,000 for serious breaches of the Data Protection Act.

The data protection powers of the Information Commissioner's Office are to:

- Conduct assessments to check organisations are complying with the Act;
- Serve information notices requiring organisations to provide the Information Commissioner's Office with specified information within a certain time period; Serve enforcement notices and 'stop now' orders where there has been a breach of the Act, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;
- Prosecute those who commit criminal offences under the Act;
- Conduct audits to assess whether organisations' processing of personal data follows good practice,
- Report to Parliament on data protection issues of concern

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's relevant responsible person – the Headmaster. Additionally, all security breaches, lost/stolen equipment or data (including remote access SecureID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the relevant responsible person – the Headmaster.