SOUTHEND HIGH SCHOOL FOR BOYS

Online Safety Policy

May 2024

For review Summer 2026

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile 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, fake news, racism, misogyny, self-harm, suicide ideology, 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

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 Governing Board

The Governing Board has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

The Governing Board 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 Governing Board will also make sure all staff receive regular online safety updates (via email, 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 Governing Board will receive reports and may have additional meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the Designated Safeguarding Lead (DSL).

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

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

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

All Governors will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2)
- 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).

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 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 Network Manager to make sure the appropriate systems and processes are in place
- Working with the Headteacher, Network 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
- Ensuring that any incidents of cyber-bullying are logged
- 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
- Undertaking periodic reviews to consider and reflect the changing risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

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 on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Ongoing monitoring of the ICT systems to ensure safety and continuity of service is maintained
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Approve and log any requests from staff to bypass filtering and monitoring for educational purposes
- Ensuring that any online safety incidents are logged on CPOMS via the Key Stage admins
- Ensuring that any incidents of cyber-bullying are investigated appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.5 All staff

All staff are responsible for:

- Understanding this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)
- 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
- Inform the Network Manager 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 and appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are reported 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.

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)

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

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.

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum 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
- Understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- Know how to report a range of concerns
- Know their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- Recognise 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 provide material to others that they would not want shared further and not to share personal material which is sent to them
- Know what to do and where to get support to report material or manage issues online
- Be aware of the impact of viewing harmful content (including extremist propaganda and exposure)

- Be aware 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
- Know that sharing and viewing indecent images of children (including those created by children) is a criminal offence that carries severe penalties including prison
- Know how information and data is generated, collected, shared, and used online
- Know 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
- Know 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)

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

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be available for parents.

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

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

6. Cyber-bullying

6.1 Definition

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

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, the school will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. The school 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.

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 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 may also send information to parents 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.

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 student's 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 the Headteacher or DSL
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

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

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

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

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

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

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

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

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

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

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

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

6.4 Artificial intelligence (AI)

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

The school recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.

The school will treat any use of AI to bully pupils in line with our published policies.

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

7. Acceptable use of the internet in school

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

8. Pupils using mobile devices in school

The pupils should follow the school mobile phone policy, published in the school diary.

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.

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)
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends

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 intended to be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the Network Manager.

10. How the school will respond to issues of misuse

Where a pupil 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 that 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.

All staff members will receive regular refresher training, as well as relevant updates as required (for example through emails, 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 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.

Governors will receive relevant training in relation to their roles, on safe internet use and online safeguarding issues periodically as part of their safeguarding training.

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

12. Monitoring arrangements

This policy will be reviewed every 2 years. At every review, the policy will be shared with the Governing Board. The review will be supported by consideration of the changing risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with other policies

This online safety policy is linked to our:

- Child protection policy
- Behaviour policy
- Anti-bullying policy

- Mobile phone policy
- Staff disciplinary procedures
- Data protection compliance statement (formerly data protection policy) and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy

Appendix 1

Student - ICT Acceptable Use Policy

Background

When you attend school, you are learning in preparation for adult life. This learning includes not only specific subject knowledge, but the development of the understanding required to be employed in a professional workplace. Our expectations in this policy are the same as those you will encounter in the workplace.

Student responsibilities

This policy outlines the acceptable use of ICT systems at Southend High School for Boys.
Our priority is to keep you safe online. You should always speak to a trusted adult if something happens to either yourself or another student which makes you feel worried, scared, or uncomfortable.

- I know that school computers and Internet access have been provided to help me with my learning and that other use of technology might not be allowed. If I am not sure if something is allowed, then I will ask a member of staff.
- I know that my use of school computers and Internet access within school will be monitored.
- I will keep my password safe and private and will avoid sharing any of my personal details online.
- I will write online messages carefully and politely, as I know they could be forwarded or seen by someone I did not intend.
- I know that bullying in any form (both online and offline) is not tolerated and that technology should not be used for bullying or harassment.
- I will refrain from taking pictures and videos of others in school.
- I will not deliberately upload or add any images, video, sounds or text that could upset, threaten the safety of or offend any member of the school community.
- I understand that it may be a criminal offence or breach of the school policy to download or share inappropriate pictures, videos, or other material online. I also understand that it is against the law to take, save or send indecent images of anyone under the age of 18.
- I will not access or change other people's files, account settings, or information.
- I will only use my phone as permitted in the mobile phone policy. This means that in lessons, I will only use my personal device/mobile phone if I have been given permission by a teacher.
- I will respect other people's information and copyright by giving a reference when using images or text from online sources.
- I will always check that any information I use online is reliable and accurate.
- I will only change the settings on the computer if a member of staff has allowed me to do so.
- I know that use of the school's ICT system for personal financial gain, gambling, political purposes, or advertising is not permitted.
- I understand that the school's Internet filtering systems are there to protect me, and I will not try to bypass them.
- If I receive an email (both internal and external) that was not meant for me, I will advise the sender immediately that I have received the email in error and I will delete it. I will not forward it on, even if I am aware of who the intended recipient is.
- I will respect the school's ICT equipment and ensure it is kept in good condition.
- If I am aware of anyone trying to misuse or damage school property, then I will report it to a member of staff.
- I know that if the school suspect that I am behaving inappropriately with technology, then enhanced monitoring and procedures may be used, such as checking and/or confiscating personal technologies such as mobile phones and other devices, and that access to the Internet may be blocked.
- I know that if I do not follow this Acceptable Use Policy, then I may incur sanctions as deemed appropriate by the school.

- I can visit websites like www.thinkuknow.co.uk www.childnet.com www.childline.org.uk www.nspcc.org.uk to find out more about keeping safe online.
- I have read and talked about these rules with my parents/carers.

Student Data Storage

Students are provided with both a Personal (N :) drive on the school network as well as access to the OneDrive cloud storage area. The school encourages students to use the OneDrive as this is secure, regularly backed up, scalable and available wherever there is an Internet connection. Students should not use USB storage devices.

Southend High School for Boys - ID Cards

The following is not permitted:

- Lending your card to others
- Borrowing someone else's card
- Using your card inappropriately
- Treating someone else's card inappropriately
- Defacing or breaking a card intentionally

Parental Responsibility

We ask that parents read this document carefully and discuss the contents with their child who will be asked to sign it during tutor time.

Parents should ensure that before being brought into school, student's personal devices have appropriate filtering and monitoring services in place.
Guidance on this can be found online: www.internetmatters.org

Student Name: Click or tap here to enter text.

Form: Click or tap here to enter text.

Date: Click or tap to enter a date.

Appendix 2

Acceptable Use Agreement and ICT Code of Conduct

As a professional organisation with responsibility for children's safeguarding it is important that all employees follow every appropriate procedure to protect data and Information Systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner.

Any infringement of this policy will be taken seriously and could result in disciplinary action and/or lead to penalties under civil or criminal law. Misuse of school ICT facilities may be a breach of the *Computer Misuse Act 1990* (https://www.legislation.gov.uk/ukpga/1990/18/contents) .

To ensure that members of staff are fully aware of their professional responsibilities when using ICT and the school systems, they are required to read and adhere to this Policy.

This Policy applies to all users of ICT facilities which are owned, leased, hired, or otherwise provided by the school as well as ICT facilities connected directly or remotely to the school's network.

This is not an exhaustive list and members of staff are reminded that ICT use should be consistent with the school ethos, appropriate school policies, relevant national and local guidance, and the Law.

Staff should be familiar with the school's E-Safety policy and Email Good Practice Guide which cover the requirements for safe use of ICT, using appropriate devices, use of social media websites and the supervision of students in the classroom.

1. Information Systems and ICT includes networks, data, and data storage, online and offline communication technologies and access devices e.g., laptops, mobile phones, tablets, digital cameras, email, and social media sites.

2. Any hardware and software provided for staff should *only* be used by them and for educational use.

3. All hardware e.g., laptops, mobile phones etc., whether used in school or taken off premises, are the property of the school, and they must be returned to the school at the request of the Network Manager or Headteacher or in the event of leaving the school's employment.

4. Do not attempt to install any purchased or downloaded software or hardware without permission from the Network Manager.

5. To prevent unauthorised access to systems or personal data do not leave any system unattended without first logging out or locking the computer.

6. Do not disclose to anyone any password or security information. Use a 'strong' password - include numbers, letters, and symbols, with 8 or more characters, preferably do not use a dictionary word. If your password is compromised, change it immediately and advise the ICT Team. Network passwords must be changed annually. If you are required to provide your password to the ICT team for maintenance on your device, you should change your password prior to hand-in or change your password on collection.

7. Ensure all personal data of students, staff or parents/carers is kept in accordance with the current data protection legislation i.e., obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary, and kept private and secure with appropriate security measures in place, whether used in the workplace, or accessed remotely.

8. Respect copyright and intellectual property rights.

9. Sensitive data should not be removed from the school site without justification and/or prior consent.

10. Do not keep or access any documents which contain school-related sensitive or personal information (including images, files, videos, emails etc.) on any personal devices unless they are secure and encrypted. Where possible use O365 (Teams) or OneDrive.

11. Do not store any personal information on any device issued by the school such as personal photographs, files, or financial information.

12. When working from home, and sharing a space with family members, ensure that your screen cannot be viewed, and information inadvertently disclosed. This also applies whilst in the school setting. For example, do not have email notifications turned on if your laptop is connected to the whiteboard.

13. Ensure any online reputation and use of ICT and information systems are compatible with professional role, whether using school or personal systems including the use of email, text, social media, gaming and any other devices or websites.

14. Do not create, transmit, display, publish or forward any material that is likely to be considered offensive, illegal, or discriminatory or could bring professional role or the school, into disrepute.

15. Report all incidents of concern regarding student's online safety to the Designated Safeguarding Lead and/or the e-Safety Coordinator as soon as possible.

16. Report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the Network Manager, Designated Safeguarding Lead and/or the e-Safety Coordinator as soon as possible. If a computer or system has been damaged or affected by a virus or other malware report this to the ICT Team as soon as possible.

17. Electronic communications with students, parents/carers and other professionals must only be made using school email addresses or telephone numbers and not personal email, social networking, or mobile phones. Any pre-existing relationships or situations that may compromise this point should be notified to the Senior Leadership team and/or Head Teacher.

18. If you receive an email (both internal and external) and are clearly not meant to be recipient, advise the sender immediately that you have received the email in error and delete it. Do not forward it on, even if you are aware of who the intended recipient is.

19. Entitlement to access your school email address will normally cease on the date of contract termination.

I understand that the school may exercise its right to monitor the use of the school's information systems, including Internet access as well as the interception of e-mails (personal and work) on work equipment, to monitor compliance with this and its safeguarding policy.

Where it believes unauthorised and/or inappropriate use has occurred, or unacceptable or inappropriate behaviour may be taking place the school will invoke its disciplinary procedure. If the School suspects that the systems may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation(s).

I agree to follow this Code of Conduct and to support the safe use of ICT throughout the school.

Full Name: …….. (printed)

Job Title: ……

Signature: …… Date: ……

Forms revised: April 2024