HEARTSACADEMYTRUST

Online Safety Policy
Including
Acceptable Use and Data Security

Reviewed	**September 2023 in line with KCSIE 2023 updates**
To be Reviewed:	**September 2026**
Version:	**v2 March 2024 (additional Prevent Duty information added)**

HEARTS Academy Trust is committed to providing a happy, caring and safe learning environment for all within a values led context, where everyone feels valued and grows in confidence and independence.

We promote HAPPINESS through a creative, exciting and practical curriculum, which generates a love of, and interest in, learning and a resilience and hope which supports us through challenging times.

Great value is placed on pupils' self ESTEEM which is developed through a positive and motivated attitude to learning, a healthy lifestyle, good social skills, self-discipline and a positive self-image.

We promote the highest standards of ACHIEVEMENT in all areas of the curriculum and help all pupils to fulfil their potential regardless of gender, race or ability.

We foster RESPECT and RESPONSIBILITY for all by establishing good relations between the school, home and community. Pupils are taught respect for themselves, others and the environment. They are also taught to take full responsibility for their own choices and responsibility for themselves and their community.

We encourage TRUTH and honesty in all aspects of school life – relationships, work and the curriculum and learn to Trust and accept others' individuality and uniqueness.

We develop SPIRITUALITY and SERVICE so that calm, quiet, reflective times which support deep thought are part of school life and beauty is appreciated. We promote a service culture that reflects our duty to support and show compassion to all members of the community and not just ourselves.

Children at the heart

1. Online Safety

It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole-school approach to online safety empowers a school to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate (KCSIE 2023, DfE).

This policy is designed to outline the Trust's intent of online safety within the curriculum, and it's work with children.

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

content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.

contact: being subjected to harmful online interaction with other users; for example: 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: online behaviour that increases the likelihood of, or causes, harm; for example, 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. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/) (KCSIE 2023, DfE).

School / Setting Wi-Fi Passwords

To be shared with authorised personnel only (e.g. Ofsted or Central Staff)

2. The Curriculum

Computing and online resources are widely used across the curriculum. Online safety is strongly embedded within our curriculum, and we continually look for new opportunities to promote it.

- The school provides opportunities within a range of curriculum areas to teach about online safety
- Educating pupils on the dangers of technologies that maybe encountered outside school is done when opportunities arise and as part of the online safety curriculum
- Pupils are taught to use technology safely, respectfully and responsibly. Through discussion and activities, they learn what is acceptable and unacceptable behaviour
- Pupils are aware of the impact of online bullying and know how to seek help if they are affected by any form of online bullying. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent, teacher/ trusted adult, or an organisation such as Childline or the CEOP report abuse button
- Pupils are taught to use search technologies effectively and appreciate how results are selected and ranked, and be discerning in evaluating digital content
- All staff are expected to incorporate online safety activities and awareness within all curriculum areas
- Our staff receive regular information and training on online safety issues from our CEOP Ambassador's training, National Online Safety and a range of external providers
- All staff receive information on the Trust Acceptable IT User Policy within the Code of Conduct as part of their induction and annual update

3. Managing the school online safety messages

- Online safety messages are embedded across the curriculum whenever the internet and/or related technologies are used
- Online safety posters/ online reminders will be prominently displayed
- Specialist visitors/facilitators work with a range of stakeholders throughout the school year, developing understanding and awareness

4. Pupils with Additional Needs

The Trust endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' online safety rules. However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of online safety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of online safety. Internet activities are planned and well managed for these children.

5. Roles and Responsibilities

The Trust will support all staff to develop their skills whilst balancing the safety and welfare of pupils and the security of our systems. All pupils are educated, as part of our curriculum, about the importance of safe and responsible uses of technology and how to protect themselves (and others) online.

All staff are responsible for their actions, conduct and behaviour when using technology at all times. Use of technology should be safe, responsible and respectful to others and at all times legal. Any misuse of technology by staff will be dealt with under the Discipline and Dismissal Procedure (Including Managing allegations of abuse against staff).

In any case giving rise to safeguarding concerns, the matter(s) will be dealt with under our child protection procedures (following our Child Protection policy – see low-level concerns reporting lines). Matters will be dealt with by the Head of School in the case of concern about the conduct of a staff member and recorded in line with our procedures and systems.

Training will be provided for all stakeholders on how to use and navigate our IT systems, particularly Google Classroom/Meet, by trained and competent school leaders. All stakeholders will feel confident to be able to safely deliver lessons and other educational content online when needed.

The Trust ensures that it's CEOP ambassadors keep abreast of current issues and guidance.

Please also refer to Keeping Children Safe in Education, our Child Protection Policy and Code of Conduct for additional information.

6. Acceptable Use of IT (including mobile devices)

Introduction

It is the aim of The Trust to create highly skilled and independent users of technology. We want all staff and children to be digitally literate (at an age-appropriate level) and able to navigate the online world with increasing skill, precision and efficiency while maintaining the utmost principles of online safety and safeguarding. We recognise that this is crucial to prepare learners for life in the modern world and for the next stage of their lives.

IT (including data) and the related technologies such as computers, email, the internet and mobile devices are an expected part of daily working life in school and the use of electronic communication and resources is encouraged.

This policy is designed to ensure that all staff are aware of their personal and professional responsibilities when using any form of IT. All staff are expected to read and understand this policy.

All members of the Trust community are expected to use IT responsibly and to comply with all applicable laws, policies and procedures, and with normal standards of professional and personal courtesy and conduct.

The Trust will take a wide and purposive approach to consider what falls within the meaning of technology. This policy relates to all technology, computing and communication devices, network hardware and software and services and applications associated with them including:

- The internet
- Email
- Mobile phones and smartphones
- Desktops, laptops, notebooks, tablets
- Personal music players (iPods or other devices)
- Devices with the capability for recording and/or storing still or moving images
- Social networking, blogging and other interactive websites
- Instant messaging (including image and video messaging apps and other forms of social media, including WhatsApp), chat rooms, blogs and message boards
- Webcams and video hosting sites (such as YouTube)
- Gaming sites and online chats through gaming
- Virtual learning environments (the GSuite for Education: Google Classroom and Google Meet, Dojo, Tapestry etc)
- SMART boards
- Other photographic or electronic equipment, including wearable technology (smart watches)

Failure to follow this policy may result in the withdrawal of access to Trust computers, email and internet and/or to disciplinary action, depending on the circumstances of the case.

Technology and the law change regularly and this policy will be updated as and when necessary. Workers will be informed when the policy has changed but it is their responsibility to read the latest version of this document.

7. Filtering and Monitoring

All staff receive appropriate safeguarding and child protection training (including online safety which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring at induction). The training is regularly updated, in addition, all staff receive safeguarding and child protection (including online safety) updates (for example, via email, safeguarding bulletins, and staff meetings), as required, and at least annually, to continue to provide them with relevant skills and knowledge to safeguard children effectively.

The designated safeguarding lead takes lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place).

Whilst it is essential that the Board of Trustees ensure that appropriate filtering and monitoring systems are in place, they are careful that "over-blocking" does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding.

Whilst considering their responsibility to safeguard and promote the welfare of children and provide them with a safe environment in which to learn, the Board of Trustees do all that they reasonably can to limit children's exposure to the above risks from the Trust's/school's IT system. As part of this process, Trustees ensure all schools have appropriate filtering and monitoring systems in place and regularly review their effectiveness. They ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified.

To support schools and colleges to meet this duty, the Department for Education has published filtering and monitoring standards which set out that schools should:

- identify and assign roles and responsibilities to manage filtering and monitoring systems.
- review filtering and monitoring provision at least annually.
- block harmful and inappropriate content without unreasonably impacting teaching and learning.
- have effective monitoring strategies in place that meet their safeguarding needs Trustees review the standards and discuss with IT staff and service providers what more needs to be done to support the Trust/schools in meeting this standard.

All staff:

- are aware of the systems in their school which support safeguarding, and these are explained to them as part of staff induction
- receive appropriate safeguarding and child protection training (including online safety which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring) which is regularly updated. In addition, all staff receive safeguarding and child protection updates (including online safety) (for example, via emails, safeguarding bulletins and staff meetings), as required, and at least annually, to provide them with the skills and knowledge to safeguard children effectively
- know the identity of the designated safeguarding lead (and any deputies) and how to contact them
- know what to do if a child tells them they are being abused or neglected. This includes understanding they should never promise a child that they will not tell anyone else about a report of abuse, as this is unlikely to be in the best interests of the child, and,
- should be able to reassure all victims that they are being taken seriously and that they will be supported and kept safe. A victim should never be given the impression that they are creating a problem by reporting abuse, sexual violence or sexual harassment, nor should a victim ever be made to feel ashamed for making a report.
- are aware that technology is a significant component in many safeguarding and wellbeing issues. Children are at risk of abuse and other risks online as well as face-to-face. In many cases abuse and other risks will take place concurrently both online and offline. Children can also abuse other children online, this can take the form of abusive, harassing, and misogynistic/misandrist messages, the non-consensual sharing of indecent images, especially around chat groups, and the sharing of abusive images and pornography, to those who do not want to receive such content.

8. **Use of School and Trust equipment/networks including Information security and access management.**
   The Trust/School is directly responsible for ensuring they have the appropriate level of security protection procedures in place in order to safeguard their systems, staff and pupil and review the effectiveness of these procedures periodically to keep up with evolving cyber-crime technologies.

Guidance on e-security is available from the National Education Network. In addition, the Trust aims to meet the Cyber security standards for schools GOV.UK. Cyber security training for school staff can be found on NCSC.GOV.UK.
Computers, mobile phones and other devices provided by the Trust are loaned to individuals to support their professional responsibilities and must be used in accordance with this policy.

Workers are responsible for the safe and proper use, care and security of equipment and systems provided. Devices must be secured appropriately especially when leaving the Trust premises (i.e., not left unattended) and protected from unauthorised access or use (i.e. not accessed by family members). Any loss, damage or unauthorised access must be reported immediately.

Workers must not use Trust equipment, networks or system to access, download, send or receive, store, create, copy or distribute any material which may be malicious, illegal, libellous, immoral, dangerous or offensive (this includes but is not limited to pornographic, sexual, violent or criminal content and racist, sexist, or otherwise discriminatory material).

Any appropriate and authorised electronic communication with pupils must be through official Trust network, channels, systems and on Trust equipment.

Permission to take, use or access trust property, including emails and website platforms, outside of the UK must be sought in writing from the Executive Headteacher.

9. Prevent Duty – in relation to online content and filtering and monitoring (read in conjunction with Child Protection policy)

Prevent Explanation and Definitions

PREVENT - Prevent is part of the UK's Counter-terrorism strategy CONTEST. The purpose of Prevent is to safeguard and support vulnerable people to stop them from becoming terrorists or supporting terrorism, as well as support the rehabilitation and disengagement of those already involved in terrorism. An explanation of PREVENT can found on pages 29-32 of CONTEST.

Prevent Duty - Section 26 of the Counter-Terrorism and Security Act (HMG, 2015) placed a duty on settings that they must, in the exercise of their functions, have 'due regard to the need to prevent people from being drawn into terrorism'. This is known as the 'Prevent Duty'.

Channel Panel - Channel is a national programme which focuses on providing support at an early stage to individuals identified as being vulnerable to being drawn into terrorism. Further information can be found within Channel and Prevent Multi-Agency Panel (PMAP) guidance (Home Office, 2021)

Key vocabulary definitions

- Extremism - the vocal or active opposition to our fundamental values, including the rule of law, individual liberty and the mutual respect and tolerance of different faiths and beliefs
- Radicalisation - refers to the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups
- Terrorism - action that endangers / causes serious violence to a person/people; causes serious damage to property; or seriously interferes with / disrupts an electronic system. Further information can be found within the Terrorism Act 2000 (legislation.gov.uk)

- **Prevent training and guidance**

  Key documents

  The Designated Safeguarding Lead should be familiar with the below key documents as they set out the responsibilities that settings have regarding PREVENT:

- Keeping Children Safe in Education (DfE, 2023) - reinforces the PREVENT duty and sets out that, similar to protecting children from other forms of harm and abuse, protecting children from radicalisation should be seen as part of the setting's wider safeguarding duties. Specific PREVENT guidance can be found under 'Preventing radicalisation' on pages 149 – 152
- Updated Prevent duty guidance: for England and Wales (Home Office, 2023)
- The use of social media for online radicalisation – a gov.uk guide for settings on how terrorist groups such as ISIL use social media to encourage travel to Syria and Iraq.

  Prevent in Essex

  The Prevent duty: an introduction for those with safeguarding responsibilities states that Designated Safeguarding Leads should be aware of the PREVENT process in their Local Authority. The information below summarises PREVENT in Essex for education settings:

- The Education Lead for Prevent in Essex is Jo Barclay, Head of Education Safeguarding and Wellbeing
- Information about the local risk and threats in Essex are disseminated to Headteachers and DSLs via the Safeguarding Forums run by the Education Safeguarding Team.
- The Essex SET Prevent policy and guidance provides an overview of PREVENT in Essex, as decided by the Prevent Delivery Group. This is a multi-agency Board with strategic oversight of Prevent in Essex which provides direction and co-ordination of the agencies that deliver on the Prevent agenda. The Education Prevent Lead attends the strategic group to represent Education
- The multi-agency Channel Panel in Essex meets on a monthly basis. It is attended by the Education Lead along with senior managers from other key agencies
- The Essex Police Prevent Team can be contacted via their website

  Responding to PREVENT concern

  If a setting has concerns about radicalisation or extremism, or if they feel a child is at risk of (or subject to) harm because of these issues, they should contact the Children and Families Hub in the first instance – as for any other safeguarding concern.

  If the Children and Families Hub feel there is a Prevent issue, they will signpost the setting to the Essex Police Prevent Team to seek advice and guidance. This team may then advise the setting to make a PREVENT referral using this referral form.

Settings are also able to discuss Prevent concerns with the Essex Police Prevent team: telephone 01245 452 196 / email prevent@essex.police.uk.

Individuals who have been referred to PREVENT may be considered at a Channel Panel meeting where the panel will decide whether to adopt the case. For support completing a PREVENT referral form, the DfE have produced guidance on Making a referral to Prevent.

10. Use of Email

Trust business must always be conducted through official email addresses, which must be secured with password controls. Workers should respond to emails during working hours in a timely and appropriate fashion. Occasionally a member of staff may choose to send emails outside of their normal working hours, but there is no obligation for emails received to be checked or responded to.

Email should be treated like any other form of written communication and, as such, the content should be appropriate and accurate and data protection compliant.

Extreme care must be taken with attachments from third parties, particularly unidentified third parties, as these may contain viruses.

Email must not be used to receive, send or forward messages that are defamatory, obscene or otherwise inappropriate. If such an email is received, whether unwittingly or otherwise and from whatever source, this must not be forwarded to any other address and must be reported immediately.

Reasonable access and use of the internet/intranet and email facilities are available to recognised representatives of professional associations' i.e., union officers for the performance of their official duties and activities.

The Trust has implemented protective measures to limit risks. All staff are expected to follow Multi-Function Authenticator (MFA) procedures to access HEARTS emails, financial platforms and web-based systems.

11. Social Networks

Social networking applications include but are not limited to:

- Blogs;
- Online discussion forums, for example, Facebook;
- Media sharing services for example YouTube;
- Professional networking sites, for example, LinkedIn;
- 'Micro-blogging' application for example Twitter.

Where the school/Trust operates official networking sites, these must be managed and used in accordance with this policy. This includes the following requirements:

- use of official (i.e., not personal) email addresses for user accounts;
- appropriate feedback and complaints information must be published in a prominent place which is easily accessible to other users;
- the school/Trust logo and other branding elements should be used to indicate the school/Trust support. The school/Trust logo should not be used on social networking applications which are unrelated to or are not representative of the school/Trust;
- users should identify themselves as their official position held within the school/Trust on social networking applications e.g., through providing additional information on user profiles;

- any contributions on any social networking application must be professional, uphold the reputation of the school/Trust and be in accordance with data protection requirements;
- users must not promote or comment on personal matters (including personal/ financial matters), commercial ventures, political matters or campaigns, religion or other matters;
- users should not respond to personal requests, abuse or questionable comments by parents or members of the public.

12. **Personal use of Trust equipment/networks**

Trust equipment, internet services, systems and email may be used for incidental personal purposes, with the approval of the line manager, provided that it:

- does not interfere with the Trust's operation of computing facilities or email services;
- does not interfere with the user's employment or performance of professional duties or other obligations to the Trust;
- is of a reasonable duration and frequency;
- is carried out in authorised break times or outside their normal working hours;
- does not overburden the system or create any additional expense to the Trust;
- is not used to access, send, receive or store inappropriate material; and
- does not bring the Trust and its community into disrepute.

Workers must notify the Trust of any significant personal use.

Reasonable access and use of the internet/intranet and email facilities is available to recognised representatives of professional associations' i.e., union officers for the performance of their official duties and activities.

Email should be treated like any other form of written communication and, as such, the content should be appropriate and accurate and data protection compliant.

Trust equipment/networks/systems must additionally not be used for

- commercial purposes not under the auspices of the Trust;
- personal financial gain;
- personal use that is inconsistent of other Trust policies or guidelines; or
- ordering of goods to be delivered to the school/Trust address or in the school/Trust's name.

13. Use of personal IT equipment in school/Trust

- Staff must secure their personal mobile phones and other devices during the school day in a locker or in a closed bag in a cupboard. All phones and other personal devices must be turned off during the school day.
- Telephones in the main school offices should be manned between 8.30 am and 3.30 pm so that urgent messages for staff can be passed on quickly.
- Mobile phones can be checked in the staff room at breaktime, lunchtime or after school.
- Once all children have left the building, staff can have mobile phones turned on and with them.
- All telephone contact with Parents/Carers from the school must be made on the school telephone and not on personal phones or from home.
- During group visits off the school site, staff may carry their own phones in bags but they should only be used in emergencies.

All photographs of children, which must only be taken using school devices, must be deleted at the earliest opportunity unless they are being collected for strategic documents, in which case parental permission

must be checked, forwarding to the School Business Manager or Office Lead for secure storage. No pictures or videos may be taken within the school or at any school-related activity, on personal devices.

- No parent is permitted to use their mobile phone whilst inside the school building or on the site. All devices should be turned off. Instructions about this will be given out at the start of school events with reminders as necessary.
- Visitors to the school must turn off their phones upon entering the building. If a contractor requires an electronic device to work in school, then an appointment must be made in advance with an appropriate member of the office or site staff.
- There may be an exception to the use of mobile phones in school in an emergency or for the continuation of business and this must be agreed upon and risk assessed by the Executive Headteacher or Head of School.

Other electronic devices

Workers should not bring other electronic devices onto school premises unless this has been specifically authorised by the Head of School. In such circumstances, the computer/equipment must be kept securely (at the risk of the owner) and security-protected so that it cannot be accessed by pupils or others at the school.

Any personal use of such equipment must be restricted to an employee's break times or outside their normal working hours and must not impact on their duties in any way.

Additionally, specific permission must be obtained prior to connecting any device to school networks/systems and the device(s) must have adequate virus protection.

Workers must ensure that no personal information regarding school/Trust business, its pupils or staff is stored on such personal equipment.

It is acknowledged that Ofsted inspectors are permitted to use electronic devices in school for the purpose of their inspection of work.

14. Personal social networks

HEARTS Academy Trust is committed to safeguarding and promoting the welfare of children and expects all staff and volunteers to share this commitment. All offers of employment are subject to the receipt of various safeguarding checks, including but not limited to online searches.

The Trust recognises individual rights to privacy and a private life. However, the law generally views social media as in the public domain, irrespective of privacy settings. Workers are therefore advised to be mindful of their duties and obligations to uphold the reputation of the Trust, to comply with the code of conduct and other policies and contractual terms in their use of personal social media – being mindful of the real possibility for material to be posted, shared and made public inadvertently or by other contacts. The Trust may require the removal of content it considers inappropriate.

It is totally unacceptable for any worker to discuss pupils, parents, work colleagues or any other member of the Trust community or any Trust-related business on any type of social networking site.

Other posting/ liking or retweeting etc on personal sites may also impact the reputation of the school/Trust or the suitability/conduct of the employee, for example, if an employee is off sick but makes comments on a site to the contrary, postings of indecent, racist, sexist, discriminatory or inappropriate images/activities etc.

Workers must not accept or propose contact, nor engage in any conversation with pupils on any personal social networking sites and should be circumspect in personal network contact with former pupils, particularly those under the age of 18 years.

Individuals working in the school should not use or access social networking sites of pupils.

Employees, volunteers, Trustees or LAB members should not name schools, the Trust or pupils, or parents on social media sites.

15. **Security**

The Trust follows sound professional practices to secure data, system programmes, email records and networks under its control.

Workers must take all reasonable precautions to maintain security and confidentiality and to protect data. This includes:

- using appropriate security measures such as encryption/password protection to transmit confidential or sensitive information;
- ensuring all devices and system access are password protected. (All laptops, memory sticks and devices used must be encrypted). Memory sticks containing data must not be removed from the Trust premises;
- ensuring that pupils are not exposed to any inappropriate images or web links; and
- respecting all copyrights and not copy, retrieve, modify or forward copyrighted materials except as permitted by the copyright owner.

The Trust has implemented protective measures to limit risks. All staff are expected to follow Multi-Function Authenticator (MFA) procedures to access HEARTS emails, financial platforms and web-based systems.

Users must not:

- use, transfer or tamper with other people's accounts and files;
- use anonymous mailing services to conceal identity when mailing through the Internet, falsify e-mails to make them appear to originate from someone else, or provide false information to any Internet service which requests name, e-mail address or other details;
- use electronic media and services in a manner that is likely to cause network congestion or significantly hamper the ability of other people to access and use the system;
- store sensitive, confidential data or photos on their own equipment – this extends to personal cameras, mobile phones and other similar devices;
- use the internet/intranet facilities or equipment to deliberately create any virus, worm, Trojan horse or any other programme that is harmful to normal computer operations.
- monitor or intercept the files or electronic communications of other workers or third parties;
- hack or obtain access to systems or accounts they are not authorised to use;
- use personal email addresses to send or receive trust information/data
- use other people's log-ins or passwords; or
- breach, test, or monitor computer or network security measures without authorisation.

Where any security breach or inappropriate connection or IT activity occurs, the user must immediately disconnect/log out and report immediately.

Breaches

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

Any policy breach by an adult is grounds for disciplinary action in accordance with the Trust Disciplinary Procedure. Policy breaches may also lead to criminal or civil proceedings.

To investigate a breach, contact the Trust IT support provider via your school office with the IP address of the machine, date and timeframe involved requesting a report form and report to the Trust Business Manager.

Incident Reporting
Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the Head of School and the Trust DPO: who can be contacted via email: dpo@heartsacademy.uk. Additionally, all security breaches, lost/stolen equipment or data (including remote access Secure ID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to your Head of School and the Trust Business Manager.

See Appendix A - flowcharts for dealing with both illegal and non-illegal incidents

Computer Viruses

- Never interfere with any anti-virus software installed on school IT equipment that you use.
- If your machine is not routinely connected to the school network, you must make provision for regular virus updates through your IT team.
- If you suspect there may be a virus on any school IT equipment, stop using the equipment and contact your IT support provider immediately. The IT support provider will advise you what actions to take and be responsible for advising others that need to know

16. **Privacy and Monitoring**

The Trust respects workers' privacy and will not routinely inspect or monitor emails, data or internet usage.

However, workers should not have any expectation of absolute privacy in his or her use of the Trust systems or equipment (including but not limited to networks/servers/internet usage/networks/Wi-Fi). Under the following circumstances the Trust reserves the right, at its discretion, to review any electronic files and messages to the extent necessary to ensure systems are being used appropriately and when required by law;

- if there is a substantiated reason to believe that a breach of the law; or Trust policy has taken place;
- if the Trust suspects that the employee has been viewing/transmitting offensive or illegal material;
- if the Trust suspects that the employee has been spending an excessive amount of time on activity which is not work-related;
- where required for compliance checks e.g., auditors, data protection; or
- where there are emergency or compelling circumstances such as staff absence.

The Trust will endeavour to notify affected individuals of any monitoring which will take place and the reason for it, save in exceptional circumstances (see below).

Workers will normally be notified of what information will be recorded and retained, for how long, who will have access and how such information will be used, which will include using such information for disciplinary purposes where applicable.

When monitoring emails, the Trust will save in exceptional circumstances; confine itself to looking at the address and heading of the emails. Workers should mark any personal emails (where these are

permitted by the Trust) as such and encourage those who send them to do the same. The Trust will avoid, where possible, opening emails clearly marked as private or personal.

The Trust considers the following to be valid reasons for checking an employee's email:

- if the employee is absent for any reason and communications must be checked for the smooth running of the Trust to continue;
- if the Trust suspects that the employee has been viewing or sending offensive or illegal material, such as material containing racist terminology or nudity (although the Trust understands that it is possible for workers inadvertently to receive such material and they will have the opportunity to explain if this is the case);
- if the Trust suspects that an employee has been using the email system to send and receive an excessive number of personal communications (or any personal emails if this is prohibited by the Trust); and
- if the Trust suspects that the employee is sending or receiving emails that are detrimental to the Trust or its pupils.

The Trust may monitor communications without notification in certain specific circumstances, including but not limited to;

- establish the existence of facts relevant to the Trust e.g., whether a contract was entered into by email;
- ascertain compliance with regulatory or self-regulatory practices e.g., checking that the Trust is complying with external or internal regulations;
- ascertain or demonstrate standards that are or ought to be achieved by workers using the system;
- investigate or detect unauthorised use of the telecommunication system, which would include checking that workers are not breaching the Trust's policy on email and internet use; and
- ensure the effective operation of the system, for example through virus monitoring.

Monitoring will be reasonable and in accordance with current legislation. CEO/Executive Headteachers approval will be required.

The Trust has a Data Retention and GDPR Policy, which will be utilised in any instances of reviewing information on workers' equipment.

Covert monitoring

The use of covert monitoring will only be used in exceptional circumstances, for example, where the Trust suspects criminal activity or where telling the employee about the monitoring would make it difficult to prevent or detect such wrongdoing.

If the Trust considers covert monitoring to be justified, this will only take place as part of a specific investigation and will cease when the investigation has been completed. CEO/Executive Headteacher approval will be required. Misuse of the facility to monitor an employee's email account will be a conduct issue and dealt with via the discipline policy.

Routine or random monitoring of equipment

Some workers have the exclusive use of mobile or fixed technology. To ensure the acceptable use of IT policy is being adhered to by all workers, the CEO/Executive Headteachers may from time to time examine individual devices. This will be by arrangement and devices will be selected at random.

16. Trust expectations for the use of TEAMS

a) All behaviour should be professional.
b) The background must be blurred, where there is a technical problem, the background must be blank.
c) If there are difficulties finding a room where you can be alone, please let the meeting lead know. Staff can use school offices if needed.
d) Attention should be paid to those sharing your space at home or at work. Where other people are likely to be in the room, please alert meeting members before the meeting. In this case, confidential information should not be discussed.
e) Unless previously agreed for the meeting to be a 'working lunch', no food should be consumed.
f) Dress should be as per the Code of Conduct.
g) General body language and behaviour should be professional and in accordance with Trust expectations.
h) Email should be used to send confidential information and TEAMS chat should not be used for this transfer.
i) No smoking throughout.
j) The screen used should reflect work and purpose, if using a second screen this should be out of view.

17. Trust expectations for remote working

- Staff will only use the Trust's email/internet/learning platforms and any related technologies for professional purposes or for use deemed appropriate and 'reasonable' by the Head of School, Executive Headteacher or Trustees.
- Staff will comply with the IT system security and not disclose any password provided to them by the Trust, School or other related authorities.
- Staff will ensure that all electronic communications with stakeholders are strictly professional.
- Staff will not give out personal details, such as mobile phone number, personal e-mail address and/or social networking identities to other stakeholders (parents/carers or pupils).
- Staff will ensure that personal data (such as data held on MIS software (i.e. Scholar Pack) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- Staff will not install any hardware, on any school machines, without the permission of the Head of School. This includes the usage of school hardware that is loaned out to pupils/families.
- Staff will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory. This includes school hardware that is loaned out to pupils/families.
- Images and/or recordings (including voice recordings) of stakeholders will only be taken using school devices, stored and/or used for professional purposes in line with the Trust policy and with the written consent of the parent, carer or staff member. Images of children will never be distributed outside the school network without the permission of the parent/carer.
- Staff will understand that all use of the Internet and digital learning platforms (and any other related technologies) can and will be monitored and logged. Data and information logged from these actions must be made available upon request and will be facilitated by the Head of School.
- Staff will respect copyright and intellectual property rights.
- Staff will ensure that online activity, both in school and outside school, will at all times remain professional and in accordance with school policy and it will not bring the Trust into disrepute.
- No stakeholder (child or parent/carer) will ever be online 1-1 with a member of school staff, at any point.
- Staff will support, promote and uphold the values set out in the Trust's online safety and data security policies and will help all stakeholders to be safe and responsible in their use of IT and related technologies.

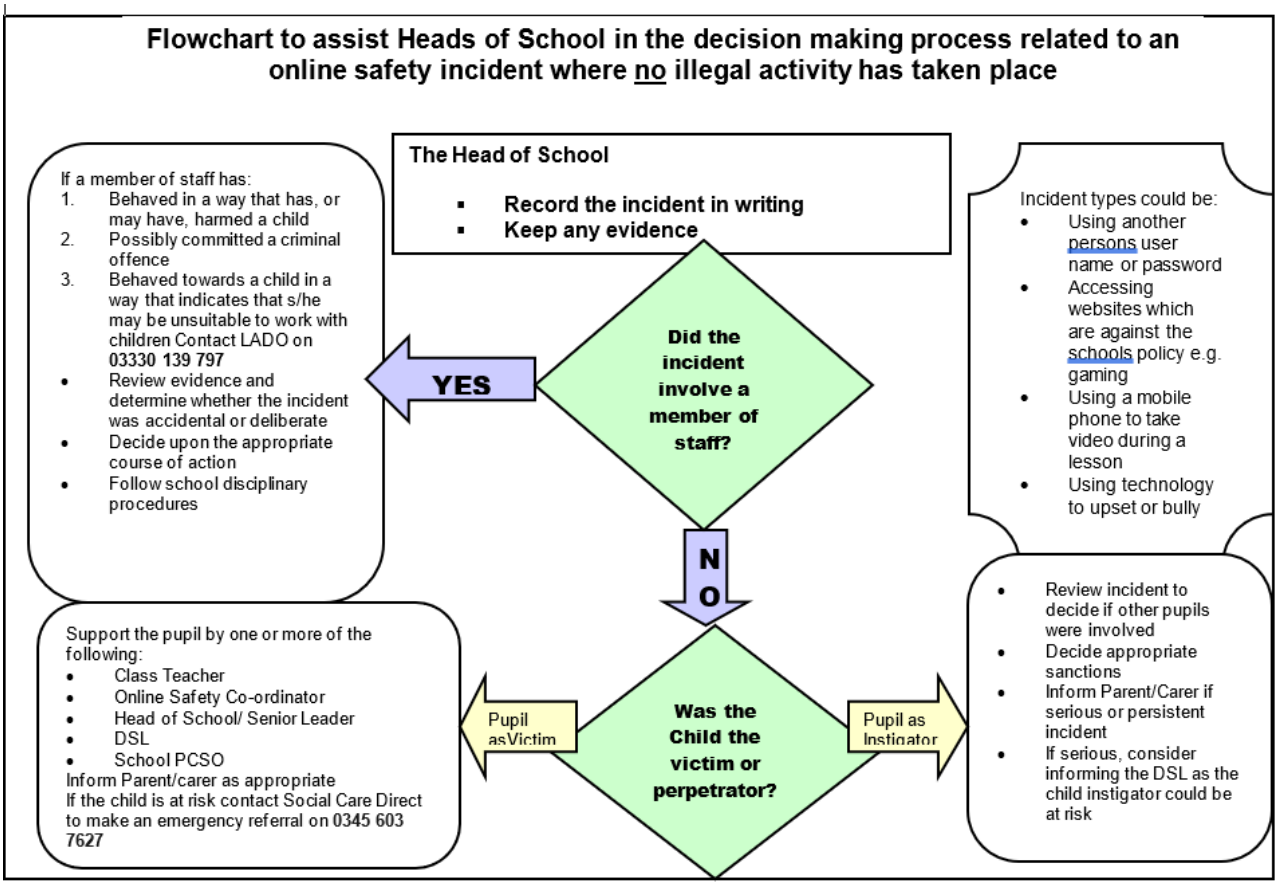
18. Disposal of Redundant ICT Equipment Policy

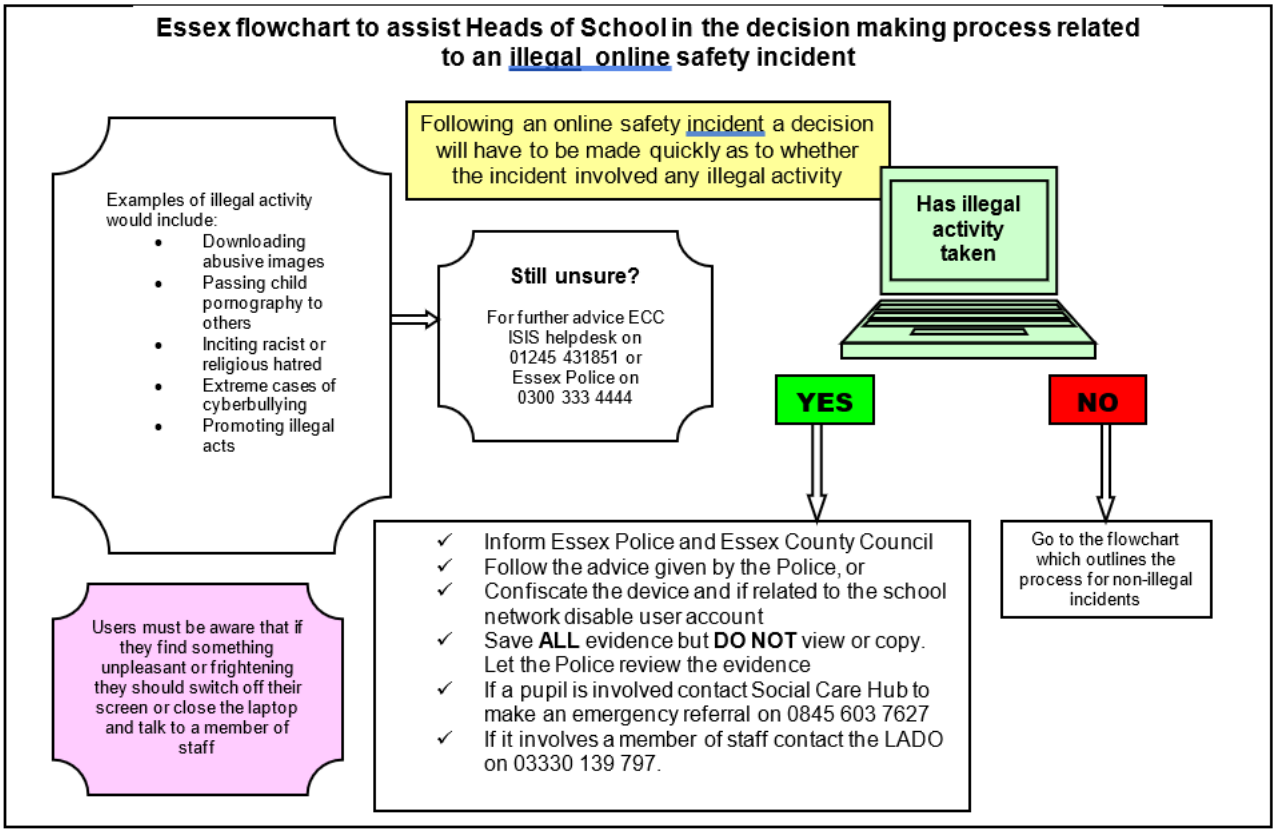
- All redundant IT equipment will be disposed of through an authorised agency as approved by the CFO / Finance Manager only. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
- All items disposed of will need to be removed from the school asset register.
- All redundant IT equipment that may have held personal data, will have the storage media over written multiple times to ensure the data is irretrievably destroyed. Or if the storage media has failed it will be physically destroyed. The Trust will only use authorised companies who will supply a written guarantee that this will happen
- Disposal of any IT equipment will conform to regulations.
- The school's disposal record will include:
  - date item disposed of
  - authorisation for disposal, including:
  - verification of software licensing
  - any personal data likely to be held on the storage media?
  - how it was disposed of e.g. waste, gift, sale
  - name of person and/or organisation who received the disposed-of item

- Any redundant IT equipment being considered for sale/gift will have been subject to a recent electrical safety check and hold a valid PAT certificate.

Note: In the Code of Conduct, Appendix D, elements of this policy feature as the Acceptable Use Agreement.

Appendix A - Flowchart to assist the Head of School in decision making





Appendix B – Useful Links

Information Commissioner website (ICO)
ICO Data Protection Act – data protection guide, including the 8 principles
IT Guidance
CEOP
Parent Info
NSPCC Net Aware
Talking pants online
Internet Matters
Keeping Children Safe in Education 2023