Online Safety Policy

Chaucer School

A member of Tapton School Academy Trust

Ratified by Governors:	May 2023
Next review due by:	May 2024
Staff Responsible:	Designated Safeguarding Lead

Contents

1. Aims

Our school aims to:

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

The four 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.

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 Education, Relationships and Sex Education (RSE) and Health 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.

The policy also takes into account the National Curriculum computing programmes of study.

This policy complies with our funding agreement and articles of association.

3. Roles and responsibilities

3.1 The Local Governing Board (LGB)

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

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The safeguarding governor oversees the online safety policy.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's IT systems and the internet (appendix 3)
- 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

- The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.
- The Headteacher is responsible for ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school's behaviour policy.

3.3 The Designated Safeguarding Lead (DSL)

Details of the school's designated safeguarding lead (DSL) and designated safeguarding deputy/deputies (DSD/DSDs) 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, IT 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 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 and dealt with appropriately in line with the school behaviour and relationships policy
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- 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
- Liaising regularly with parents/carer to ensure they understand expectations

This list is not intended to be exhaustive.

3.4 The IT Network Manager

The IT Network Manager and their team is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis 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
- Conducting full security checks and monitoring the school's IT systems ongoing throughout each day
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that all logged online safety incidents are dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.5 The Online Safety Link Governor

The Safeguarding Governor is the Online Safety Link Governor and is responsible for:

- Approving this policy and strategy and subsequently review its effectiveness, e.g. by asking the questions in the helpful document from the UK Council for Child Internet Safety (UKCIS) Online safety in schools and colleges: Questions from the Governing Board
- Asking about how the school has reviewed protections for pupils in the home (including when with online tutors) and remote-learning procedures, rules and safeguards (see remotesafe.lgfl.net for guidance to policies and an infographic overview of safeguarding considerations for remote teaching technology.
- Ensuring an appropriate senior member of staff, from the school or college leadership team, is appointed to the role of DSL with lead responsibility for safeguarding and child protection (including online safety) with the appropriate status and authority and time, funding, training, resources and support.
- Supporting the school in encouraging parents and the wider community to become engaged in online safety activities
- Having regular strategic reviews with the online-safety coordinator / DSL and incorporate online safety into standing discussions of safeguarding at governor meetings
- Working with the DPO, DSL and headteacher to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information

3.6 The LIFE Curriculum Lead

The LIFE curriculum lead is responsible for:

- Embedding consent, mental wellbeing, healthy relationships and staying safe online into the PSHE / Relationships education, relationships and sex education (RSE) and health education curriculum. This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers will address online safety and appropriate behaviour in an age appropriate way that is relevant to their pupils' lives.
- Complementing the computing curriculum, which covers the principles of online safety at all key stages, with progression in the content to reflect the different and escalating risks that pupils face. This includes how to use technology safely, responsibly, respectfully and securely, and where to go for help and support when they have concerns about content or contact on the internet or other online technologies.
- Working closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE / RSE.
- Including and maintaining an up to date RSE policy on the school website.
- Working closely with the Computing subject leader to avoid overlap but ensure a complementary whole-school approach, and with all other lead staff to embed the same whole-school approach

3.7 The Computing Curriculum Lead

The Computing Curriculum Lead is responsible for:

- Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum
- Work closely with the RSHE lead to avoid overlap but ensure a complementary whole-school approach
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements

3.8 The Communications Officer

The Communications Officer is responsible for:

- Monitoring online safety alerts in school
- Maintaining an awareness of current online safety issues.
- Identifying any online safety issues that impact our students, staff and parent/carers directly.
- Reporting any online safety concerns relating to Chaucer School, its staff, pupils or their families to the appropriate organisation or CEOP.
- Communicating online safety issues to parents and the wider school community through the school's website and social media channels

3.9 The Online Safety Team

The Online Safety Team at Chaucer School is made up of the following roles within the school. The Designated Safeguarding Lead

The Online Safety Coordinator

The Communications Officer

The LIFE Curriculum Lead

The Computing Lead

The IT Network Manager

The Online Safety Coordinator chairs regular working groups to ensure compliance and information sharing across everyone with a role in Online safety at Chaucer school.

3.10 All staff and volunteers

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

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

3.11 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 IT systems and internet (appendices 1 and 2)

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

3.12 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

4. Educating pupils about online safety

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

All schools have to teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

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 which 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)

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

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

5. Educating parents about online safety

The school's DSL in conjunction with the school's Communication Officer will raise parents' awareness of internet safety in communications home, meetings and in information via our website and social media. This policy will also be shared with parents.

Online safety will also be covered during parents' evenings.

The school will let parents 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 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 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour and relationships policy.)

6.2 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.

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. Teachers will discuss cyber-bullying with their class(es).

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 also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour and relationships 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 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, the authorised staff member will:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff
- 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 cooperation

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 /deputy headteacher 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 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 and relationships policy

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

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 to 3). 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, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1 to 3.

8. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them.

Any mobile devices that are seen or heard by staff in school will be confiscated and returned to the pupil at 3.30pm at the end of a 30 minute detention.

Any breach of the acceptable use agreement by a pupil, particularly where criminal activity is suspected, may trigger disciplinary action in line with the school's behaviour and relationships policy and mobile phone policy, which may result in the confiscation of their device for a longer period of time, in order to plan for further action. In this case parent/carers will be informed of the length of time the device will be confiscated for and the actions that will be taken.

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 (following Trust password policy of at least 8 characters, at least 1 capital letter and at least 1 number.
- Ensuring their hard drive remains secure through the hard drive encryption process 2022/23– 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
- Keeping operating systems up to date by always installing the latest updates. Please speak to the IT team if you are unsure how to do this and want them to apply the updates.

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

Work devices must be used solely for work activities.

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

10. How the school will respond to issues of misuse

Where a pupil misuses the school's IT systems or internet, we will follow the procedures set out in our policies on behaviour and relationships, and acceptable usage of IT. 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 IT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with staff code of conduct/disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

11. Training

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

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

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

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

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure 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 DSDs will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

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

Volunteers will receive appropriate training and updates, if applicable.

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

12. Monitoring arrangements

The DSL, DSDs, Communications Officer, Pastoral teams, and all staff can log behaviour and safeguarding issues related to online safety.

This policy will be reviewed every year by the DSL. At every review, the policy will be shared with the governing board. The review will be supported by an annual risk assessment that considers and reflects the

risks 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 and safeguarding policy
- Behaviour and relationships policy
- Mobile phone policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy
- Code of Conduct

Appendix 1: Secondary student acceptable use agreement (students)

STUDENT ACCEPTABLE USE FOR ONLINE SAFETY AND SOCIAL NETWORKING STANDARDS
This applies to school devices and personal devices being used in school and also school/Trust owned devices being used at home I will • only access the school's IT systems and Internet via my own username and password. • keep my password safe and not share it with other people. • ask the IT team to check any attachments or links before I click on them if I don't know that they are safe. • if given permission to use my own device in school ask the IT team to check the device I want to link to the school IT before I do it to make sure there are no viruses. • follow guidelines for safe use of the Internet. • report any materials or conduct which I feel is unacceptable to the Teacher or IT Team. • only use my own device in school if I have permission. • immediately report any IT damage or faults. I will not • damage school IT on purpose. • download IT viruses on purpose. • play computer games during the school day unless I have been directed to do so by a teacher. • alter or delete another person's files. • use chat rooms and social networking sites during the school day. • put personal information on-line (this could include names, addresses, email, telephone numbers, age, gender, educational details, financial details etc). • do anything online which is offensive, hurtful or otherwise upsetting to another person. • post anonymous messages or forward chain letters. • use inappropriate language. • take, publish or share pictures or videos of anyone without their permission. • use school IT for personal use without a teacher's permission. • copy someone else's school work and pretend it is my own. • access inappropriate materials such as pornographic, racist or offensive material. • install or attempt to install or store programmes on any school device. • try to alter computer settings. • will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others. • use any programs or software that might allow me to bypass the filtering/security systems. I understand that • school will monitor my use of the systems, devices and digital communications. School may share this information with my parents/carers, the police or other agencies depending upon the severity of the incident. School may check my school documents for viruses and unsuitable material at any time. • if I use my own devices in the school, I will follow the rules set out in this agreement. • I am responsible for my actions, both in and out of school. • the school also has the right to take action against me if I am involved in an incident out of school (examples would be cyber-bullying, use of images or personal information).
I have read and understood the above statements and I agree to the rules for use of ICT facilities and the Internet. I understand that deliberate failure to do this could result in the loss of my access rights to IT along with further sanctions if there was serious misuse.

Student signature.....Form.....

Student full name.....Date.....

This agreement will be re-issued annually, and access to systems will be revoked unless this is returned to the school.

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

STAFF ACCEPTABLE USE FOR ONLINE SAFETY AND SOCIAL NETWORKING STANDARDS

- I will read and comply with the ***Trust's Data Protection Policy.***
- All data stored by TSAT staff is the property of TSAT and should not be removed when staff leave.
- I will not disclose my username or password to anyone.
- I will not write down or store a password unsecurely.
- I will always log off the computer when I have finished and lock it when unattended.
- I will never use anyone else's login, email address or password.
- I will not use my personal email or personal phone number as a contact for students.
- I will never use my personal email address for work.
- When communicating electronically with students or parents it will only be via the school's accredited systems.
- I will ensure that all communication is transparent and open to scrutiny.
- I will ensure that communication with students is in a professional manner.
- I understand that the use of the network or any school device to knowingly access inappropriate materials is strictly forbidden and may constitute a criminal offence.
- I will report any accidental access to unacceptable material immediately to my manager and notify my manager if I suspect someone else of misusing ICT. I will also inform the Designated Safeguarding Lead if misuse may be a child protection issue.
- I will ensure that students under my supervision use ICT facilities and the Internet appropriately to support learning. I will challenge and report any misuse.
- I will ensure the ICT team have screened all devices for malicious software before connecting to the network and take care when opening unknown email attachments. I will seek advice from the ICT team if I am unsure about the safety of any such devices or attachments.
- I will make sure that if I need to transport personal data of any kind I will do so using an encrypted external device that has a password in line with the ***Trust's Data Protection Policy.***
- I will not attach any devices to the network that may contain files that breach copyright, GDPR or other laws.
- I agree to use the school's ICT only for work related use during my directed working hours.
- If I use a work mobile device or laptop at home and in school, I will not access inappropriate applications/ Internet searches (including gambling).
- I will take all reasonable steps to ensure the safety of ICT which I take off site and will remove anything of a personal nature before it is returned to school.
- My mobile device (phones, tablets, smart wear) will be turned off or kept on silent mode during lessons except if required to authenticate with school network login or email, or in an emergency situation with the agreement of a member of the Senior Leadership Team.
- Employees should not access personal emails or messages during directed working hours except in an emergency situation with the agreement of a member of the Senior Leadership Team.
- I will only photograph or video students on school devices as part of a planned learning activity or, in exceptional circumstances, for identification purposes and will ensure footage is only used with the correct consent.
- I will not photograph or video students on personal devices.
- If I choose to have my school email account configured on my personal mobile device, I will set a 6-digit passcode and install the school Microsoft Intune email policy application and accept the agreement**.**
- I understand that the Trust monitors Internet usage and sites used by staff. All inappropriate searches are automatically alerted to the DSL and Headteacher.
- I understand that the misuse of ICT facilities and the Internet could result in disciplinary action being taken.
- I will follow Trust password policy of: At least 8 characters, At least 1 capital letter, at least 1 number.
- When working from home I will not leave any school system logged in unattended, these include remote

access, Bromcom, SharePoint and video conferencing meetings or training.

Online Learning and Meetings - including Teams and Zoom

To find out how to do any of the below please visit the Trust Knowledge Base site to access useful guides - https://tsat.sharepoint.com/sites/tsat/policies/KnowledgeBase

- When using Teams always blur your background when providing online lessons, recording online content, or attending a meeting when outside of school.
- When using Zoom for a meeting whilst outside of school always upload and apply a custom background.
- Only use scheduled meetings setup in your Teams/Zoom calendar with students or meeting attendees.
- Make sure you end the meeting when meeting with students (or meetings attendees) and do not just leave.
- Always set the lobby option to 'Only me' (organiser) in Teams and enable the Waiting Room in Zoom for all external meetings and lessons so that you know who you is attending, and you can admit each person to the meeting.
- Always set the who can present option to 'Only me' (organiser) for all lessons with students. In Zoom you need to change the share screen advanced sharing options for who can share to 'Only Host' (organiser). Its optional whether you want to do this for meetings with adults in Teams/Zoom.
- If recording a meeting, always make sure the attendees are aware and they are happy for you to record the meeting, if they are not then do not record. Once you start the recording state that the meeting is being recorded and participants have consented to it. *"Please note that any attempt to covertly record such a meeting may be considered as gross misconduct".*
- When entering a meeting/lesson you should always seek to ensure that your camera and microphone is active so that the person leading the meeting/lesson is made aware of your presence.
- If there are any issues with the use of camera (i.e., WIFI or data issues) then you should make the person/s leading the meeting/lesson aware of this.
- Any use of message chat should be to appropriately contribute to the meeting/lesson taking place. It should be the person/s leading the meeting who decide if the message chat needs to be shared on the screen to support the meeting.

Staff social networking standards

Below sets out the standards expected of all staff when using social media.

DO

- Always act responsibly. Even if you do not identify your profession or place of work, your conduct could jeopardise any professional registration and/or your employment.
- Be considerate to your colleagues. Pictures or information about colleagues should not be posted on social networking sites unless you have the agreement of the individual.

DO NOT

- Share confidential information online.
- Build or pursue relationships with pupils even when the pupil has left the Trust.
- Use social networking to inform professional practice without careful consideration and discussions with management.
- Discuss students, parents, colleagues, School or Trust in a way which may be deemed inappropriate or damage reputation.
- Post pictures of students/families online even if they have asked you to do this.
- Take pictures of parents, carers, or students without the relevant consents.
- Raise concerns about your work online. If you have concerns, then these should be discussed with your line manager.
- Engage in activities online which may bring the Trust into disrepute.

- Be abusive, bully, derogatory, defamatory, or offensive.
- Employees may not use social networking sites or other unauthorised sites during directed working hours.

All the above applies to open and private sections of social networking sites.

Appendix 3: Online safety training needs – self-audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with an online safety concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	