The Rowan Learning Trust

Three Towers
An Alternative Provision Academy
Expanding Horizons

Online Safety Policy

Adopted: February 2024
Review: At least annually in line with reviews to all Safeguarding Policies

1 Aims

Three Towers (TTAPA) aims to:

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

The 4 key categories of risk

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

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

2 Legislation and Guidance

This policy is based on the Department for Education's (DfE) 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 learners' electronic devices where they believe there is a 'good reason' to do so.

Our filtering and monitoring systems fully comply with the Department for education's Digital and Technology Standards. We do not publish specific details of this to protect the integrity of our systems and networks. Meeting digital and technology standards in schools and colleges - Filtering and monitoring standards for schools and colleges - Guidance - GOV.UK (www.gov.uk)

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

3 Roles and Responsibilities

3.1 The Trust will ensure that each school has appropriate filtering and monitoring systems in place on school devices and networks, and that their effectiveness is regularly reviewed**.** They will review the DfE filtering and monitoring standards, and discuss with key staff including the headteacher and service providers what needs to be done to support each 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.

3.2 The local governing committee (LGC) has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation. The LGC will:

- ensure that all staff undergo online safety training as part of child protection and safeguarding training;
- ensure staff understand their expectations, roles and responsibilities around filtering and monitoring;
- ensure all staff receive regular updates (via email, briefings and meetings) as required and at least annually so that they are continually provided with the relevant skills and knowledge to effectively safeguard children;
- co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL);
- ensure children are taught how to keep themselves and others safe, including keeping safe online;
- nominate a governor to oversee online safety.

The nominate governor is the Chair of Governors.

All governors will:

- ensure that they have read and understand this policy;
- agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (Appendix 3);
- ensure that online safety is a running and interrelated theme while devising amnd implementing their whole school 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 learners with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

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

3.4 Core Leadership Team

Details of our DSLs are set out in our Safeguarding and Child Protection Policy.

The assistant headteacher (AHT) responsible for our digital strategy and who is our data protection lead also has 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 LGC 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 networks;
- working with the Trust's Director of Operations and ICT Manager, as well as the school's IT technician to make sure that the appropriate systems and processes are in place;
- working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents;
- working with the DSL 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 policy;
- updating and delivering staff training on online safety (see 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 committee;
- undertaking regular (at least annual) risk assessments that consider and reflect the risks children face;
- with the DSL providing regular safeguarding and child protection updates, including online safety, to all staff at least annually in order to provide them with relevant skills and knowledge to safeguard effectively.

This list is not intended to be exhaustive.

3.5 The Trust ICT manager

The Trust ICT manager is responsible for:

- putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure learners 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.

Together with our ICT technician:

- conducting a full security check and monitoring the school's ICT systems regularly on a proactive basis and reactively as needs/situations arise;
- blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files;
- ensuring that any online safety incidents are logged and dealt with appropriately within this policy;
- ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school's Anti-Bullying and Behaviour & Relationships Policies.

This list is not intended to be exhaustive.

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

- reading and maintaining an understanding of this policy;
- implementing this policy consistently;
- knowing that the AHT working with the DSL, is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing using CPOMS and informing ithelpdesk@ttapa.net;
- agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (Appendix 3);
- following the correct procedures by seeking permission from a member of CLT to request access to educational sites if they need to bypass the filtering and monitoring systems for educational purposes;
- ensuring that learners follow the school's terms on acceptable use;
- working with the AHT and/or 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 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 and carers 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.

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

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

3.7 Visitors and members of the community who use our CT systems or internet will be made aware of this policy, when relevant, and are expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

4 Educating Learners about online safety

All schools have to teach:

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

We recognise that our learners have had a disrupted educational experience and will therefore have considerable gaps in their knowledge and skills. Many of our learners are also vulnerable and therefore it is even more important that we address their individual learning needs as well as working to ensure that they meet as many of the national expectations for the end of their phase of education as possible.

Key Stage 1 learners mostly attend on a part time basis on a short-term intervention place. Most are dual registered with their mainstream school or if they are single registered quickly have a new mainstream school identified for them, so we work closely with their school to ensure that the learners are taught to:

- use technology safely and respectfully, keeping personal information private;
- identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

Key Stage 2

Some Key Stage 2 learners attend on a part time basis on either an intervention place or a medical needs place for a short period. They remain dual registered with their mainstream school, so we work closely with their school to ensure collective we meet their learning needs regarding online safety.

Our full time Key Stage 2 learners remain with us until a permanent placement has been found. During their time with us we work to fill any gaps in their knowledge and skills to ensure learners know how to:

- use technology safely, respectfully and responsibly;
- recognise acceptable and unacceptable behaviour;
- identify a range of ways to report concerns about content and contact.

Through the PSHE curriculum our primary learners are taught the following topics throughout the year

- keeping safe - including information on:
    - age restrictions with respect to gaming, social media, films and videos;
    - keeping personal information safe and strategies for keeping safe online;
    - how to report on any concerns.
- friendships/Relationships online - including information on:
    - building up relationships and communicating effectively online;
    - online/cyber-bullying;
    - privacy and personal boundaries.
- media literacy and digital resilence including information on:

- ways in which the internet and social media can be used positively and negatively;
- how data is used and shared online;
- how information can be manipulated or invented.

We recognise that our learners have had a disrupted primary education experience and we will endeavour to ensure that by the **end of primary school**, learners should know:

- that people sometimes behave differently online, including by pretending to be someone they are not;
- that the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous;
- the rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them;
- how to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met;
- how information and data is shared and used online;
- what sorts of boundaries are appropriate in friendships with peers and others (including in a digital context);
- how to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.

Key Stage 3

Some Key Stage 3 learners attend on a part time basis on a medical needs place for a short period. They remain dual registered with their mainstream school, so we work closely with their school to ensure collective we meet their learning needs regarding online safety.

Our full time Key Stage 3 learners remain with us until a permanent placement has been found. During their time with us we work to fill any gaps in their knowledge and skills to ensure learners know how 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.

Key Stage 4

Some Key Stage 4 learners attend on a part time basis on a medical needs place for a short period. They remain dual registered with their mainstream school, so we work closely with their school to ensure collective we meet their learning needs regarding online safety.

Our full time Key Stage 4 learners usually remain with us until the end of Y11. During their time with us we work to fill any gaps in their knowledge and skills to ensure learners know how to:

- understand how changes in technology affect safety, including new ways to protect their online privacy and identity;
- report a range of concerns.

We recognise that our learners have had a disrupted primary education experience and we will endeavour to ensure that by the **end of secondary school**, learners should 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 learners with SEND.

Learners will be taught about online safety as part of the curriculum.

Our curriculum is devised to meet the personalised needs of learners when they are referred to us. For dual-registered learners we try to complement the curriculum delivered in their other school.

5 Educating parents/carers about online safety

We raise parents'/carers' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents on our website – www.ttapa.net

Online safety will also be covered during parents' meetings. We let parents/carers know

- what systems we use to filter and monitor online abuse;
- what their child is being asked to do online, including any sites they have been 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 their child's pastoral manager.

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

6 Cyber-bullying

6.1 Definition

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

6.2 Preventing and addressing cyber-bullying

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

We actively discuss cyber-bullying with learners, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. Staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying, including 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 learners, as part of safeguarding training (see section 11 for more detail).

The school also shares information 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, we follow the processes set out in our Anti-Bullying Policy. Where illegal, inappropriate or harmful material has been spread among learners, 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 grounds to suspect possessing that material is illegal. They will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

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

- poses a risk to staff or learners, 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 learners and staff. If the search is not urgent, they will seek advice from the headteacher, or their deputy;

- explain to the learner why they are being searched, how the search will happen, and give them the opportunity to ask questions about it;
- seek the learner's cooperation.

Authorised staff 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 member of staff in conjunction with the DSL and the headteacher or their deputy 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 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 learner 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 learners 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 & Relationships Policy.

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

6.4 Artificial intelligence (AI)

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

TTAPA recognises that AI has many uses to help children learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography - pornographic content created using AI to include someone's likeness.

We will treat any use of AI to bully learners in line with our Anti-Bullying and Behaviour & Relationships 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 learners, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of our ICT systems and the internet.

Visitors are expected to read and agree to our terms on acceptable use if relevant.

Use of our 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 learners, 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, 2 and 3.

8 Learners using mobile devices in school

Learners are not permitted to bring any into school. There is guidance about our approach to Learner Mobile Phone use on the website.

Any use of mobile devices (eg tablets, mobile phones and smart watches) in school by learners must be in line with the acceptable use agreement (see appendices 1 and 2).

Any breach of the acceptable use agreement by a learner may trigger disciplinary action in line with our 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 in line with the Trust's policy;
- ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device;
- ensuring the device locks if left inactive for a period of time;
- not sharing the device among family or friends;
- installing anti-virus and anti-spyware;
- keeping operating systems up to date by bringing the device into school at least once each half term and connecting to the network so that routine updates can be installed.

Staff members must not use the device in any way which would violate the school's terms of acceptable use.

Work devices should be used solely for work activities in line with rowan Learning Trust Policies.

If staff have any concerns over the security of their device, they must seek advice from the ICT team – using ithelpdesk@rlt.education

10 How the school will respond to issues of misuse

Where a learner misuses our ICT systems or internet, we will follow the procedures set out in our policies. 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 our ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be discussed with the Trust's Director of People and then dealt with in accordance with recommendations and relevant Trust/school policy. 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

11.1 All Staff:

- as part of their induction receive training on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.
- receive refresher training at least once a year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).
- are 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 learners can recognise dangers and risks in online activity and can weigh the risks up;
- develop the ability to influence learners to make the healthiest long-term choices and keep them safe from harm in the short term.

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

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

11.4 Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our Safeguarding & Child Protection Policy.

12 Monitoring arrangements

Staff log behaviour and safeguarding issues related to online safety using CPOMS and ARBOR.

This policy will be reviewed annually by the AHT responsible for our digital strategy. At every review, the policy will be shared with the LGC. The review (such as the one available here) is supported by regular risk assessment that considers and reflects the risks learners 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:

- *RLT Data Protection Policies*
- *RLT Social Media Policy*
- *RLT Staff Code of Conduct*
- *RLT Staff Disciplinary Procedures*
- *RLT & TTAPA ICT and internet acceptable use policy*
- *RLT & TTAPA Privacy notices*
- *TTAPA Behaviour & Relationships Policy*
- *TTAPA Complaints Policy*
- ***TTAPA Safeguarding & Child Protection Policy***

UNICEF - UNCRC

The UN Convention of the Rights of the Child sets out human rights of every person under 18 and applies to every child without discrimination, whatever their ethnicity, gender, religion, language, abilities or any other status, whatever they think or say, whatever their family background (Article 2). Articles directly relating to this policy are:

3 (Best interests of the child)	17 (Access to information from the media)
5 (Parental guidance and a child's evolving capacities)	19 (Protection from violence, abuse and neglect)
6 (Life, survival and development)	31 (Leisure, play and culture)
8 (Protection and preservation of identity)	34 (Sexual exploitation)
9 (Separation from parents)	35 (Abduction, sale and trafficking)
11 (Abduction and non-return of children)	36 (Other forms of exploitation)
12 (Respect for the views of the child)	37 (Inhumane treatment and detention)
13 (Freedom of expression)	38 (War and armed conflicts)
14 (Freedom of thought, belief and religion)	40 (Juvenile justice)
15 (Freedom of association)	41 (Respect for higher national standards)
16 (Right to privacy)	42 (Knowledge of the rights of a child)

Appendix 1: Acceptable Use Agreement for Learners in KS1

ACCEPTABLE USE OF THREE TOWERS' ICT SYSTEMS AND INTERNET: AGREEMENT FOR LEARNERS AND PARENTS/CARERS	
Name of learner:	

When I use the school's ICT systems (like computers) and get onto the internet in school I will:
• Ask a teacher or adult if I can do so before using them
• Only use websites that a teacher or adult has told me or allowed me to use
• Tell my teacher immediately if:
  ○ I click on a website by mistake
  ○ I receive messages from people I don't know
  ○ I find anything that may upset or harm me or my friends
• Use school computers for school work only
• Be kind to others and not upset or be rude to them
• Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
• Only use the username and password I have been given
• Try my hardest to remember my username and password
• Never share my password with anyone, including my friends.
• Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
• Complete my work through TEAMS assignments
• Check with my teacher before I print anything
• Log off a computer when I have finished using it
 	
I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.	

Signed (learner):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for learners using the school's ICT systems and internet, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 2: Acceptable Use Agreement for Learners in KS2, KS3 and KS4

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR LEARNERS AND PARENTS/CARERS	
Name of learner:	
I will read and follow the rules in the acceptable use agreement policy **When I use the school's ICT systems (like computers) and get onto the internet in school I will:** • Always use the school's ICT systems and the internet responsibly and for educational purposes only; • Only use them when a teacher is present, or with a teacher's permission; • Keep my username and passwords safe and not share these with others; • Keep my private information safe at all times and not give my name, address • or telephone number to anyone without the permission of my teacher or parent/carer; • Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others; • Always log off or shut down a computer when I'm finished working on it. **I will not:** • Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity; • Attempt to download any outside media (software, music, videos, games etc) onto school computers; • Open any attachments or follow any included links, without first checking with a teacher; • Use any inappropriate language when communicating online, including in emails; • Log in to the school's network using someone else's details, or share their details online; • Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision. **If I bring a personal mobile phone or other personal electronic device into school:** I will place it in my locker when I arrive and collect it when I leave at the end of the session. **I understand and agree that the school will monitor the websites I visit and that there will be consequences if I do not follow the rules.**	
Signed (learner):	**Date:**
Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for learners using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 3: Acceptable Use Agreement for Staff, Governors, Volunteers & Visitors

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS,VOLUNTEERS AND VISITORS	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material); • Use them in any way which could harm the school's reputation; • Access social networking sites or chat rooms; • Use any improper language when communicating online, including in emails or other messaging services; • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network; • Share my password with others or log in to the school's network using someone else's details; • Take photographs of learners without checking with teachers first; • Share confidential information about the school, its learners or staff, or other members of the community; • Access, modify or share data I am not authorised to access, modify or share; • Promote private businesses, unless that business is directly related to the school.	
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I understand and agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL), member of CLT and ICT technician know if a learner informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly and ensure that learners in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 4: 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 learners can abuse their peers online?	
Do you know what you must do if a learner approaches you with a concern or issue?	
Have you completed keeping children safe online training within the last 3 years?	
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 learners 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?	