Coast and Vale

WHERE LEARNERS AND STAFF THRIVE

Trust Policy

Online Safety Policy

Approver: Trustees
Review Cycle: Annual

Revision History			
Date	**Version**	**Short Description of Changes**	**Approved by:**
Oct 2023	V1.0	Policy adopted	Trustees
Nov 2024	V1.1	No changes	Trustees

This Policy Applies To:
Secondary Schools
Primary Schools
Centralised Trust Employees
Trustees & Governors

Document Management Information

Applicable to:	All settings, all staff
Development and Consultation:	Trust IT Manager, Trust SLT & Safeguarding Colleagues
Dissemination:	To be disseminated via Every for staff to read, available on the Staff Hub and website. Parents will be notified by school it has been updated via BromCom.
Implementation:	In the delivery and implementation of IT services for learners and staff.
Training:	Staff receive regular safeguarding training. Online Safety will be embedded into this.
Review Frequency:	Annual
Based on:	v1.0
Policy Author:	Service Delivery Manager
Executive Policy Owner:	CEO
Approval by:	Trustees
Version:	1.1
Approval Date:	20 November 2024
Next Review Due:	November 2025

If you require this policy in a more accessible format please contact the Trust Compliance Officer on compliance@coastandvale.academy

Executive summary text for current policy version:

This policy is to ensure the safety of our learners in any of our school settings.

No changes have been made to the policy.

Contents

1 Introduction

1.1 Coast and Vale Learning Trust understands that using online services is an important aspect of raising educational standards, promoting learner achievement, and enhancing teaching and learning. The use of online services is embedded throughout Trust schools; therefore, there are several controls in place to ensure the safety of learners and staff.

1.2 The breadth of issues classified within online safety is considerable, but they can be categorised into four areas of risk:

1.2.1 **Content**: Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, self-harm and suicide, and discriminatory or extremist views.

1.2.2 **Contact**: Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children.

1.2.3 **Conduct**: Personal online behaviour that increases the likelihood of, or causes harm, e.g. sending and receiving explicit messages, and cyberbullying.

1.2.4 **Commerce**: Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

1.3 The measures implemented to protect learners and staff revolve around these areas of risk.

1.4 This policy has been created with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all our learners and staff. Staff are also issued with the Acceptable Usage Policy which covers staff specific elements.

2 Responsibilities

2.1 The Trust is the employer and therefore accountable for IT provision and security and ensuring overall compliance with statutory requirements. The Trust has appointed a Chief Executive Officer (CEO) to oversee all aspects of the Trust including Information Technology and Safeguarding.

2.2 Responsibilities of the Trust Board

2.2.1 Ensure that there is an effective policy in place for Online Safety and that this is documented and implemented throughout the Trust.

2.2.2 Ensuring that this policy is effective and complies with relevant laws and statutory guidance.

2.2.3 Ensuring the DSL's remit covers online safety.

2.2.4 Reviewing this policy on an annual basis, inline with Keeping Children Safe in Education.

2.2.5 Ensuring their own knowledge of online safety issues is up to date by undertaking training.

2.2.6 Ensuring all staff undergo safeguarding and child protection training, including online safety.

2.3 Responsibilities of the CEO

2.3.1 The CEO holds overall responsibility for Information Technology and Online Safety at the Trust. To support the CEO with their duties, specific responsibilities have been assigned to designated roles in the Trust team and to the Head or Principal of each school.

2.4 Responsibilities of the Chief Operating Officer (COO)

2.4.1 Carry out the duties as delegated by the CEO.

2.4.2 Ensure any areas of non-compliance raised by either the Head/Principal, LGC or the Trust Compliance Officer are managed to mitigate the risks effectively and efficiently.

2.5 Responsibilities of Trust SLT

2.5.1 Ensure that Heads/Principals are fully aware of the Online Safety Policy and how this relates to their learners.

2.6 Responsibilities of the Designated Safeguarding Lead

2.6.1 Taking the lead responsibility for online safety in the school.

2.6.2 Acting as the named point of contact within the school on all online safeguarding issues.

2.6.3 Undertaking training so they understand the risks associated with online safety and can recognise additional risks that learners with SEND face online.

2.6.4 Liaising with relevant members of staff on online safety matters, e.g. the SENDCo and the IT Services Management Team.

2.6.5 Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.

2.6.6 Ensuring safeguarding is considered in the school's approach to remote learning.

2.6.7 Ensuring appropriate referrals are made to external agencies, as required.

2.6.8 Working closely with the police during police investigations.

2.6.9 Keeping up to date with current research, legislation and online trends with termly meetings with the Trust IT Manager and Service Delivery Manager.

2.6.10 Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by learners and staff.

2.6.11 Ensuring all members of the school community understand the reporting procedure.

2.6.12 Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.

2.6.13 Monitoring online safety incidents to identify trends and any gaps in the school's provision and using this data to update the school's procedures.

2.6.14 Reporting to the Local Governing Committee about online safety

2.7 Responsibilities of the Trust IT Manager

2.7.1 Ensure the security of the network against cyber security threats.

2.7.2 Ensure that all Trust devices are connected to the network and adhere to the Trust's policies and security measures.

2.7.3 Ensure that there is an appropriate level of monitoring and filtering in place to ensure that learners are not exposed to material that is in inappropriate.

2.7.4 To meet termly with DSLs to review current practices and trends

2.7.5 Maintain a secure Wi-Fi network with filtered access to the internet

2.7.6 Ensure the adequate reporting of IT risks and incidents are made in a timely manner to the COO.

2.7.7 To manage IT staff and ensure that the IT service fully satisfies the security and safeguarding requirements of the Trust.

2.7.8 To provide access to resources to blocked sites and software only if required for the delivery of education or for staff job roles (e.g. unblocking of social media)

2.7.9 To only add software/apps or allow access to websites if they have no risk to the end user or where there is data sharing have been risk assessed inline with UK GDPR and the Data Protection Act 2018

2.7.10 Ensure that there is a disaster recovery plan in place and back ups available if there is a cyber security incident.

2.8 Responsibilities of the Head/Principal of each school.

2.8.1 The Head/Principal is responsible for the implementation of the Trust's IT, Data Protection policies and associated procedures; however, the legal responsibility and accountability will remain with the CEO. The Headteacher/Principal may delegate the day to day operations within their school to another senior member of staff while retaining overall responsibility.

2.8.2 Ensure that online safety is a running and interrelated theme throughout the school's policies and procedures, including in those related to the curriculum, teacher training and safeguarding.

2.8.3 Supporting the DSL and the deputy DSL by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.

2.8.4 Ensuring staff engage with the Trust's mandatory cyber security and online safety training.

2.8.5 Supporting staff to ensure that online safety is embedded throughout the curriculum so that all learners can develop an appropriate understanding of online safety.

2.8.6 Communicate regularly with parents to reinforce the importance of children being safe online.

2.9 Responsibilities of the Local Governing Committee

2.9.1 Ensure the school is adhering to Trust policies and procedures.

2.10 Responsibilities of IT Services Staff

2.10.1 That incidences of learners bypassing online security are reported appropriately and quickly to ensure that they are actioned.

2.10.2 To collect information for investigations as needed.

2.10.3 Ensure backups are checked

2.11 Responsibilities of All Employees & Volunteers

2.11.1 All staff should also follow the Acceptable Usage Policy.

2.11.2 Adhere to the information, instructions and training that they have received regarding Online Safety.

2.11.3 Do not attempt to circumnavigate filtering or access sites that are blocked.

2.12 Learners are responsible for:

2.12.1 Adhering to the Acceptable Use Agreement and other relevant policies.

2.12.2 Seeking help from school staff if they are concerned about something they or a peer have experienced online.

2.12.3 Reporting online safety incidents and concerns in line with the procedures within this policy

3 Educating Learners

3.1 Learners will be taught about online safety as part of the curriculum. The text below is taken from the National Curriculum computing programmes of study.

3.2 Primary schools

3.2.1 In Key Stage 1, learners will be 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

3.2.2 Learners in Key Stage 2 will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

3.2.3 By the end of primary school, learners will 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

3.3 Secondary

3.3.1 In Key Stage 3, learners 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

3.3.2 Learners 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

3.3.3 By the end of secondary school, learners 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)

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

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

4 Educating Parents

4.1 The Trust's schools will raise parent's awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.

4.2 Online safety will also be covered during parents' evenings.

4.3 The school will let parents know:

4.3.1 What systems the school uses to filter and monitor online use

4.3.2 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

4.3.3 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.

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

5 Cyber-bullying

5.1 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.

5.2 Cyberbullying can include, but is not limited to, the following:

5.2.1 Threatening, intimidating, discriminatory or upsetting messages

5.2.2 Threatening or embarrassing media sent via electronic means

5.2.3 Silent or abusive phone calls or using the victim's device to harass others, to make them think the victim is responsible

5.2.4 Unpleasant or defamatory information/comments/messages posted online

5.2.5 Abuse between young people in intimate relationships online

5.3 Cyberbullying against learners or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Anti-bullying Policy and Child Protection Policy

6 Child-on child sexual abuse and harassment

6.1 Learners may also use the internet and technology as a vehicle for sexual abuse and harassment. Staff will understand that this abuse can occur both in and outside of school and off and online and will remain aware that learners are less likely to report concerning online sexual behaviours, particularly if they are using systems that they know adults will consider to be inappropriate for their age.

6.2 The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

6.2.1 Threatening, facilitating or encouraging sexual violence

6.2.2 Voyeurism and Upskirting

6.2.3 Sexualised online bullying

6.2.4 Unwanted and unsolicited sexual comments and messages

6.2.5 Consensual or non-consensual sharing of sexualised imagery

6.2.6 Abuse between young people in intimate relationships online

6.3 All staff will be aware of and promote a zero-tolerance approach to sexually harassing or abusive behaviour, and any attempts to pass such behaviour off as trivial or harmless. Staff will be aware that allowing such behaviour could lead to a school culture that normalises abuse and leads to learners becoming less likely to report such conduct.

6.4 Staff will be aware that creating, possessing, and distributing indecent imagery of children, i.e. individuals under the age of 18, is a criminal offence, even where the imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves.

6.5 The school will be aware that interactions between the victim of online harmful sexual behaviour and the alleged perpetrator(s) are likely to occur over social media following the initial report, as well as interactions with other learners taking “sides”, often leading to repeat harassment. The school will respond to these incidents in line with the Child-on-Child Addendum to Keeping Children Safe in Education.

6.6 The school responds to all concerns regarding online child-on-child sexual abuse and harassment. Concerns regarding online child-on-child abuse are reported to the DSL, who will investigate the matter in line with the Child Protection Policy.

7 Grooming and exploitation

7.1 Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.

7.2 Staff will be aware that grooming often takes place online and that learners who are being groomed are commonly unlikely to report this behaviour for many reasons.

7.3 Due to the fact learners are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse. The DSL will ensure that online safety training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming are, including but not limited to:

7.3.1 Being secretive about how they are spending their time.

7.3.2 Having an older boyfriend or girlfriend, usually one that does not attend the school and whom their close friends have not met.

7.3.3 Having money or new possessions, that they cannot or will not explain.

8 Child sexual exploitation (CSE) and child criminal exploitation (CCE)

8.1 Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a learner may be groomed online to become involved in a wider network of exploitation.

8.2 CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet.

8.3 Where staff have any concerns about learners with relation to CSE or CCE, they will bring these concerns to the DSL without delay, who will manage the situation in line with the Child Protection Policy.

9 Radicalisation

9.1 Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment, e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda. Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.

9.2 Staff members will be aware of the factors which can place certain learners at increased vulnerability to radicalisation. Staff will be expected to exercise vigilance towards any learners displaying indicators that they have been, or are being, radicalised.

9.3 Where staff have any concern about any learners relating to radicalisation, this should be reported.

10 Mental Health

10.1 The internet, particularly social media, can be the root cause of a number of mental health issues in learners, e.g., low self-esteem and suicidal ideation.

10.2 Staff will be aware that online activity both in and outside of school can have a substantial impact on a learner's mental state, both positively and negatively. The DSL will ensure that training is available to help ensure that staff members understand popular social media platforms and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a learner is suffering from challenges in their mental health.

11 Online Hoaxes and Trends

11.1 For the purposes of this policy, an “online hoax” is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online social media platforms.

11.2 For the purposes of this policy, “harmful online challenges” refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media channels and daring others to do the same. Although many online challenges are harmless, an online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly as a result of partaking in the challenge itself or indirectly as a result of the distribution of the video online – the latter will usually depend on the age of the learner and the way in which they are depicted in the video.

11.3 Where staff suspect there may be a harmful online challenge or online hoax circulating amongst learners in the school, they will report this to the DSL immediately.

11.4 The DSL will conduct a case-by-case assessment for any harmful online content brought to their attention, establishing the scale and nature of the possible risk to learners.

11.5 The DSL and headteacher will only implement a school-wide approach to highlighting potential harms of a hoax or challenge when the risk of needlessly increasing learners’ exposure to the risk is considered and mitigated as far as possible, this approach may also involve engaging with parents and carers.

12 Acceptable Internet Use

12.1 Learners, staff and other members of the school community are only granted access to the school’s internet network once they have read and agreed to the Acceptable Use Agreement.

12.2 All members of the school community are encouraged to use the school’s network, instead of mobile networks, as the network has appropriate filtering and monitoring to ensure individuals are using the internet appropriately for their age group. The Acceptable Usage form for Primary school learners is Appendix 1 and for Secondary and post-16 learners Appendix 2 of this policy and for staff is part of the Staff Acceptable Usage Policy.

12.3 Use of the Trust's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual’s role.

12.4 Internet traffic is monitored and any inappropriate access will be flagged.

13 Monitoring and filtering

13.1 The Trust's network and devices use age-appropriate filtering and has monitoring systems in place that does not lead to unreasonable restrictions as to what learners can be taught with regards to online teaching and safeguarding.

13.2 The Trust DSL's and IT Manager will determine what filtering and monitoring systems are required by the school. The systems implemented are appropriate to learners' ages, the number of learners using the network, how often learners access the network, and the proportionality of costs compared to the risks.

13.3 The Trust IT Services Team are responsible for monitoring the filtering and monitoring systems to ensure they are effective and appropriate.

13.4 Change requests for the filtering system are directed to the IT Services Team via the Service Desk and must be approved before being actioned. Reports of inappropriate websites or materials are made to the IT Services Team immediately, who will investigate the matter and makes any necessary changes.

13.5 Deliberate breaches of the filtering system are reported to the DSL and IT Services Team who will escalate the matter appropriately. If a learner has deliberately breached the filtering system, they will be disciplined in line with the Behavioural Policy.

13.6 The Trust's network and Trust-owned devices are appropriately monitored. All users of the network and Trust-owned devices are informed about how and why they are monitored. Concerns identified through monitoring are reported to the DSL who manages the situation in line with the Child Protection Policy.

14 Use of devices in the classroom

14.1 A wide range of technology is used during lessons, including laptops, iPad's, Chromebooks, desktop PC's and cameras.

14.2 Learners must be supervised when using technology and/or online materials during lesson time –this supervision is suitable to their age and ability.

14.3 Learners should be taught to treat devices with respect and caution. Damage done to devices should be taken seriously and in line with the school's Behaviour Policy.

14.4 Damage to devices should be reported immediately to the IT Services Team so it can be assessed.

14.5 Learners should not eat/drink near devices.

14.6 Learners should not use a staff device when it is logged into their profile. Staff permissions and learner permissions are different with staff having more access to systems.

14.7 Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that learners use these platforms at home, the class teacher should always review and evaluate the resource as well as following the Data Protection Impact Assessment process if this is a new system.

14.8 Class teachers ensure that any internet-derived materials are used in line with copyright law. If staff are unsure about the suitability of resource, they should contact the IT Services Team or Trust Compliance Officer.

15 Examining Devices

15.1 Learners should not use mobile phones or electronic devices during school hours. They will be confiscated if discovered.

15.2 In the case of an investigation, access to a learners personal device may be required in order for the investigation to be conducted. This will only be done if there are reasonable grounds to do so, i.e.

- There is a risk posed to staff or learners, and/or
- An item identified in the school rules as a banned item for which a search can be carried out is involved, and/or
- There is evidence in relation to an offence

15.3 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 DSL or other applicable member of staff
- 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 learners cooperation

15.4 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.

15.5 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

15.6 If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL to decide on a suitable response. If there are

images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

15.7 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 learner and/or the parent/carer refuses to delete the material themselves

15.8 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 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

15.9 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

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

Appendix 1: Acceptable Use Agreement – Primary School Learners

Agreement / online-safety rules

- I will only use IT equipment in school for school purposes
- I will only use my class e-mail address or my own school e-mail address when e-mailing
- I will only open e-mail attachments from people I know, or who my teacher has approved
- I will not tell other people my passwords
- I will only open/delete my own files
- I will treat IT equipment carefully and not attempt to damage or break it.
- I will make sure that all IT contact with other children and adults is responsible, polite and sensible
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately
- I will not give out my own/others details such as name, phone number or home address. I will not arrange to meet someone or send my image unless this is part of a school project approved by my teacher and a responsible adult comes with me
- I will be responsible for my behaviour when using IT equipment because I know that these rules are to keep me safe
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community
- I know that my use of IT can be checked and my parent/carer contacted if a member of school staff is concerned about my safety
- I will not sign up for any online service unless this is an agreed part of a school project approved by my teacher

---

Dear Parent/ Carer

IT including the internet, e-mail and mobile technologies has become an important part of learning in our school. We expect all children to be safe and responsible when using any IT resource

Please read and discuss these online -safety rules with your child and return the slip at the bottom of this page. Please take care to ensure that appropriate systems are in place at home to protect and support your child/ren.

Parent/ carer signature

We have discussed this document with …….. (child's name) and we agree to follow the online-safety rules and to support the safe use of ICT during my child's time.

Signed (parent/Carer): Date:

Print name:

Appendix 2: Acceptable Use Agreement - Secondary and Post 16 Learners

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

When I use the school's IT systems (like computers or laptops) and get onto the internet in school I will:

- Always use the school's IT 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 usernames and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- 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've finished working on it
- Treat IT resources respectfully and do not damage them on purpose
- Do not eat or drink when using a computer
- Report something wrong with IT equipment immediately to the teacher

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
- Use a personal device for internet access during the school day
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

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 (pupil): Date:

Parent/carer's agreement: I agree that my child can use the school's IT 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:

Print name: