TAPESTRY LEARNING PARTNERSHIP

Pupil/Student Online Safety Policy

Department:	Education
Policy Owner:	Head of IT/Director of Safeguarding & SEND
Date of issue:	April 2026
Date revised:	
Next review date:	April 2027

Revision History

Version	Date	Author	Summary of changes

Contents

1.0 Introduction 4
2.0 Aims 5
3.0 Roles and Responsibilities 5
4.0 Curriculum and provision 6
5.0 Parental engagement 7
6.0 Loan devices 7
7.0 Filtering & monitoring 8
8.0 Trips 8
9.0 Cyber security 9
10.0 Response to issues of misuse 9
11.0 Inclusion and equity 10
Appendix A 11
Appendix B 12

1.0 Introduction

Children, young people and adults interact with technologies such as mobile phones, games consoles and the internet daily on a multitude of platforms and experience a wide range of opportunities, attitudes and situations. These opportunities can greatly enhance our way of sourcing information and learning about the world around us, but can occasionally place children, young people and adults in danger.

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

Content: being exposed to illegal**,** inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
Contact: being subjected to harmful online interaction with other users, for example: peer to peer abuse, 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, for example: making, sending and receiving explicit images e.g. consensual and non-consensual sharing of nudes and semi-nudes and/pornography, sharing other explicit images and online bully: and
Commerce: risks such as online gambling, inappropriate advertising, phishing and financial scams.
Tapestry Learning Partnership (Tapestry) has a 'Duty of Care' to protect all our staff, children and young people, and visitors from these dangers, with the support of parents/carers and other members of the community.

The purpose of this online safety policy is to outline what measures Tapestry and its schools/academies take to ensure that everyone can work in a safe environment and that any online safety issue is detected and dealt with in a timely and appropriate way.

This document is intended for public consumption as well as that of staff, parents/carers and local community and is a clear outward statement on Tapestry's online safety practices.

It is important that we strike the right balance between controlling access to the internet and technology, setting rules and boundaries and educating children and young people, staff and parents/carers about responsible use. We are aware that children and young people and staff cannot be completely prevented from being exposed to risks both on and offline. Our children and young people need to be empowered and educated so that they are equipped with the skills to make safe and responsible decisions as well as to feel able to report any concerns.

All members of staff must be aware of the importance of good online safety practice in the classroom in order to educate and protect the children and young people in their care. Members of staff also need to be informed about how to manage their own professional reputation online and demonstrate appropriate online behaviours compatible with their

role. This policy should be read in conjunction with the Acceptable Use of IT, Staff Behaviour Policy, Safeguarding Policy.

2.0 Aims

- Have robust processes in place to ensure the online safety of the whole school/academy community
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school/academy community in its use of technology, including mobile and smart technology
- Ensure that all children and young people have age-appropriate knowledge and skills to keep themselves safe when online
- Ensure that parents/carers are kept informed and supported regarding online safety
- Ensure that all staff have necessary knowledge and skills to educate children and young people about online safety and skills to keep themselves safe when online

3.0 Roles and Responsibilities

Governors:

Ensure that schools/academies are including online safety in its curriculum

School Senior Leadership Team:

Ensure that all year groups are being taught online safety as per their curriculum plan
Monitor impact of curriculum online safety education through discussions with children and young people and staff keeping records of incidents, related actions, audits and adjust the curriculum to respond effectively to online safety concerns within the academy.
Ensure that all staff understand their responsibilities
Ensure that there are opportunities for parents/carers to be kept fully informed and supported

All Staff:

Have clear understanding of online safety issues and required actions
Report any online safety concerns/issues to their Senior Leadership Team as soon as the issue is identified
Take responsibility for their own actions using the internet and communication technologies, adhering to the Trust's related policies, including the Data Protection and Acceptable Use of IT policies, at all times

Teachers:

Planning and carrying out age-appropriate online safety lessons
Reinforcing this learning throughout the year
Responding to children's questions/concerns

Children and young people:

Engage with online safety learning opportunities
Report any online safety concerns/issues to a member of staff, or parent – whether they occur in school or outside
Take age-appropriate responsibility for their own actions when using the internet and communication technologies adhering to Tapestry related policies, including the Acceptable Use of IT policies, at all times.

IT Support & Specialist staff:

- Ensure that appropriate technological solutions are in place to ensure online safety as well as possible whilst still enabling children and young people to use the internet effectively in their learning.
- Ensure that all information captured using these systems is secure, accessible to the appropriate members of staff, and stored safely. In addition, securing and preserving evidence of any online safety breaches.
- Ensure the technology systems which track internet use to detect online safety breaches are working and maintained.
- Assists in the resolution of online safety issues.

Designated Safeguarding Lead:

Takes responsibility for understanding the filtering and monitoring systems and processes in place.

Regularly reviews the system in place and responds to any safeguarding concerns that are identified through ICT misuse.

4.0 Curriculum and provision

Each school/academy will ensure that it delivers a robust online safety curriculum. That is taught to every year group as part of the computing curriculum,as well as throughout the year as part of other subjects as and when the use of Digital Technologies is used in the classroom, including the safe use of social media and the internet.

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

Primary children will be taught:

- Use technology safely, respectfully, responsibly and securely, 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
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact
- Be discerning in evaluating digital content

Secondary children and young people will be taught:

- 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
- 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

5.0 Parental engagement

Schools will raise parents/carers' awareness of internet safety by communicating information via their website or parental engagement platforms.

Online safety will also be covered during parents/carers' evenings.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use
- What their children and young people are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child or young person will be interacting with online

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the Designated Safeguarding Lead (DSL).

For additional information and support see Appendix A.

Concerns or queries about this policy can be raised with the DSL or the headteacher.

6.0 Loan devices

Tapestry understands the importance of children and young people being able to use the internet for education and personal development. This includes personal laptops, social media platforms, games, and apps.

Under certain circumstances Tapestry may provide children and young people with a laptop for their studies, under the condition of it being used for educational purposes, accessing appropriate resources only.

Tapestry also recognises that safeguards need to be in place to ensure children and young people are always kept safe.

When using Tapestry loaned devices, the Acceptable User Policy and Safeguarding Policy still apply.

Tapestry will ensure all devices are:

- Filtered and monitored at all times
- Device access and software installation is limited

Parents/carer must ensure that they:

- Know what filtering and monitoring systems are in place
- Have read and discuss the loan agreement Appendix B with their child or young person and then sign it and return it.
- Understand and have engaged with the additional resources regarding online safety Appendix A
- Report any concern as soon as possible to the school/academy's DSL

7.0 Filtering & monitoring

Tapestry uses many different technologies to help to ensure online safety for the whole Tapestry community.

- Tapestry will use internet filtering to block inappropriate content and in addition block websites which are irrelevant to the child and young person's programme of study and are considered time wasting or counterproductive to the learning environment.
- Tapestry uses systems which can track all activity on Tapestry computers. This system will help flag potential online safety issues which will be monitored and then can be investigated by senior staff.
- Tapestry will restrict which activities children and young people can perform using ICT and the internet through systems security policy and access controls to the networks we operate.

School staff will work with the IT team to use control mechanisms to attempt to limit the applications and web sites which the students can visit whilst using ICT within a lesson.

- DSL's will actively monitor the use of ICT activity using the school's filtering and monitoring systems which can flag potential online safety issues.
- DSL's will periodically review internet access logs to track any websites which could potentially present an issue.
- DSL's will periodically review internet and network logs to track trends and use the information to look at ways of improving online safety.
- Teaching staff will directly monitor the use of ICT and internet use in the classroom and flag concerns to the DSL's and the ICT team and work with them to record and action any concerns.

8.0 Trips

For trips/events away from school/academy, staff must ensure they use a issued a "trip mobile" phone use this for any authorised or emergency communications with children and young people/students and parents/carers. If deviation from this policy (e.g. by mistake or because the "trip mobile" phone did not work) occurs staff must notify the

Headteacher/Principal immediately. If the use of a personal mobile phone is required in an emergency staff will ensure that the number is hidden to avoid a parent/carer or child/young person accessing a personal and private phone numbers.

Residentials and trips are an considered an extension of school/academy and therefore this policy still applies offsite while the children and young people are under the care of school staff.

If children and young people are required to connect to another organisation's Wi-Fi/network, staff must be aware that other connections may not be as well controlled (e.g. via filtering and monitoring) as the network and systems in school/academy and therefore staff must compete a risk assessment prior to using external facilities.

School/academy staff are responsible for risk assessing and managing such situations. Staff should seek advice from the DSL where necessary.

9.0 Cyber security

Where a cyber-attack may compromise any processing of data/information in school/academy, Tapestry has a Cyber Response Plan implemented to mitigate the impact of a Cyber Security incident.

In the event of a cyber-attack, the Trust will:

- Act swiftly and decisively with the Head of IT, to mitigate the impact.
- Isolate affected systems to prevent the spread of the attack
- Back up data
- Ensure the backups are held offline
- Ensure systems for restoring services and recovering data from the backups are tested and reliable
- Advise the National Cyber Security Centre (NCSC)
- Advise the local law enforcement and Action Fraud
- Inform the Department for Education by emailing: securityenquiries@education.gov.uk

For exams and assessments, any work completed in an exam situation is stored in a secure location which is not accessible from outside Tapestry and only by designated staff members internally.

10.0 Response to issues of misuse

Whenever a child and young person or staff member infringes the online safety policy the incident will be fully investigated by a senior member of staff and an appropriate sanction applied. Staff incidents will be investigated and action taken as per Tapestry's Staff Disciplinary, Capability, Grievance and Appeals Policy and related procedures.

Incidents involving children and young people will be dealt with sensitively but firmly, with parents/carers fully informed. Issues such as use of non-educational sites during lessons will be dealt with by the class teacher using their school/academy's behaviour

sanctions. More serious issues such as using the internet to search for inappropriate content, sending unauthorised unkind messages to other children and young people, deliberately deleting other child and young person's work or damaging equipment will be referred to senior staff for investigation and action.

In significant cases such behaviour could lead to suspension, permanent exclusion or police involvement. Tapestry will involve police and/or other safeguarding professionals if it is appropriate to do so.

11.0 Inclusion and equity

Tapestry strongly believes that all children and young people should have full and equal access to all learning opportunities and experiences. It is the responsibility of all staff to ensure that children and young people are supported and challenged as appropriate to their individual need.

Appendix A

Working with Parents/carers and the Community

Tapestry believes that the use of information and communication technologies brings great benefits across the curriculum. Clearly many children and young people will also have access to ICT and the internet at home, often without some of the safeguards that are present within the school environment. Therefore parents/carers/carers must often be extra vigilant about their child's e-safety at home.

Highlighting E-Safety issues and setting out our plans to ensure appropriate, effective and safer use of electronic communications aims to support a safe and structured learning experience for our children and young people.

One of the goals of Tapestry is to support parent's role in providing an e-safe environment for their children to work in outside school/academy.
Useful e–Safety programmes include:

Think U Know: www.thinkuknow.co.uk

Childnet: www.childnet.com

Kidsmart: www.kidsmart.org.uk

Orange Education: www.orange.co.uk/education

Safe: www.safesocialnetworking.org

E-Safety Contacts and References

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk

Childline: www.childline.org.uk

Childnet: www.childnet.com

Click Clever Click Safe Campaign: http://clickcleverclicksafe.direct.gov.uk

Cybermentors: www.cybermentors.org.uk

Digizen: www.digizen.org.uk

EiS - ICT Support for Schools and ICT Security Advice: www.eiskent.co.uk

Internet Watch Foundation (IWF): www.iwf.org.uk

Kidsmart: www.kidsmart.org.uk

Teach Today: http://en.teachtoday.eu

Think U Know website: www.thinkuknow.co.uk

Virtual Global Taskforce — Report Abuse: www.virtualglobaltaskforce.com

Appendix B

[Date]

Dear Parent/Carer,

RE: Online Safety Agreement

Tapestry Learning Partnership understands the importance of children and young people being able to use the internet for education and personal development. This includes personal laptops, social media platforms, games, and apps.

We have provided your child/young person with a laptop for their studies, and we aim to support our children and young people in making use of these appropriately.

However, we also recognise that safeguards need to be in place to ensure children and young people are always kept safe.

There are 4 main areas we promote with children and young people around online safety, and we would like to share them with you.

Content – This can be words/images posted online that can be harmful, inappropriate, or illegal. This can also include pornography, fake news, racism, misogyny and radicalisation.

Contact – The risk of harm with our children and young people interacting with people online, that may pose as children or with intention of grooming young people.

Conduct – This refers to the way people behave online, and may include bullying, or sending and receiving nude images online.

Commerce – This is around protection from inappropriate advertising, gambling, or financial scams.

It is important that as parents/carers you are aware of these risks and have regular conversations with your child to ensure that they are safe online.

This agreement is part of our overarching **code of behaviour for children and young people and staff and volunteers.** It also fits with our overarching **online safety policy** and **safeguarding policy** all of which can be found on our website.

If you would like to know more about this, please speak to [Staff Name] – [Role] – [School Contact Details]

Child or Young person: Please read the following agreement and discuss it with your parents/carers.

Parents/carers: Please read and discuss this agreement with your child/young person and then sign it, asking your child/young person to sign it too, and return it to [Staff Name] by [Date].

If you have any questions or concerns, please contact the school/academy's Designated Safeguarding Lead.

Child/Young person's agreement

- I will be responsible for my behaviour when using the internet, including social media platforms, games, and apps. This includes the resources I access and the language I use.
- I will not deliberately browse, download, or upload material that could be considered offensive or illegal.
- If I accidentally come across any such material, I will report it immediately to my parent/carer or teacher at school/academy.
- I will not send anyone material that could be considered threatening, bullying, offensive or illegal.
- I will not give out any personal information online, such as my name, phone number or address.
- I will not reveal my passwords to anyone.
- I will not arrange a face-to-face meeting with someone I meet online unless I have discussed this with my parents/carers, and I am accompanied by a trusted adult.
- If I am concerned or upset about anything I see on the internet or any messages that I receive, I know I can talk to [ ] .
- I understand that my internet use at [ ]will be monitored and logged onsite.
- I understand that I have a responsibility when using the device at home to adhere to the expectations highlighted in this agreement.
- I understand that these rules are designed to keep me safe and that if I choose not to follow them, the school/academy may contact my parents/carers and/or appropriate services.

Signatures:

We have discussed this online safety agreement and [ ] agrees to follow the rules set out above.

Parent/carer signature.....

Date .....

Child/young person signature.....

Date .....

Further Support for Parents/carers

https://www.nspcc.org.uk/keeping-children-safe/online-safety/

https://saferinternet.org.uk/guide-and-resource/parents/carers-and-carers