



Online Safety Policy

Bespoke Learning Ltd.



Contents:

Statement of intent

1. [Legal framework](#)
2. [Roles and responsibilities](#)
3. [Managing online safety](#)
4. [Cyberbullying](#)
5. [Child-on-child sexual abuse and harassment](#)
6. [Grooming and exploitation](#)
7. [Mental health](#)
8. [Online hoaxes and harmful online challenges](#)
9. [Cyber-crime](#)
10. [Online safety and the curriculum](#)
11. [Use of technology in the classroom](#)
12. [Use of smart technology](#)
13. [Filtering and monitoring online activity](#)
14. [Emails](#)
15. [Generative artificial intelligence \(AI\)](#)
16. [Social networking](#)
17. [Bespoke Learning Ltd.'s website](#)
18. [Remote learning](#)
19. [Monitoring and review](#)

Statement of intent

Bespoke Learning Ltd understands that using online services is an important aspect of raising educational standards, promoting pupil achievement, and enhancing teaching and learning. Students may use a computer in a public library or they may use a laptop provided by Bespoke Learning Ltd. Their use will always be supervised.

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

- **Content:** Being exposed to illegal, inappropriate or harmful material, for example:
 - Pornography.
 - Racism.
 - Misogyny.
 - Self-harm.
 - Suicide.
 - Discrimination.
 - Radicalisation.
 - Extremism.
 - Misinformation.
 - Disinformation, including fake news.
 - Conspiracy theories.
- **Contact:** Being subjected to harmful online interaction with other users, for example:
 - Peer to peer pressure.
 - Commercial advertising.
 - Adults posing as children or young adults with the intention to groom or exploit children 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 messages.
 - Consensual and non-consensual sharing of nudes and semi-nudes.

- Sharing of pornography.
- Sharing other explicit images.
- Online bullying.
- **Commerce:** Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The measures implemented to protect pupils will revolve around these areas of risk.

Bespoke Learning Ltd. has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and teachers.

1. Legal framework

This policy has due regard to all relevant legislation and statutory guidance including, but not limited to, the following:

- Online Safety Act 2023
- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2025) 'Filtering and monitoring standards for schools and colleges'
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2025) 'Keeping children safe in education 2025' (KCSIE)
- DfE (2023) 'Teaching online safety in school'
- DfE (2022) 'Searching, screening and confiscation'
- DfE (2025) 'Generative artificial intelligence in education'
- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2024) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people (updated March 2024)'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'

- National Cyber Security Centre (2020) 'Small Business Guide: Cyber Security'

This policy operates in conjunction with the following Bespoke Learning Ltd. policies:

- Allegations of Abuse Against staff Policy
- Technology Acceptable Use Agreement
- Child Protection and Safeguarding Policy
- Anti-Bullying Policy
- Pupils' Personal Electronic Devices Policy
- Teacher Code of Conduct
- Behaviour Policy
- Confidentiality Policy
- Device User Agreement
- Staff ICT and Electronic Devices Policy
- Prevent Duty Policy
- Remote Education Policy

2. Roles and responsibilities

Dawn Griffiths, Director of Bespoke Learning Ltd. will be responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the DSL's remit covers online safety.
- Reviewing this policy on an annual basis.
- Ensuring their own knowledge of online safety issues is up-to-date.
- Ensuring all teachers undergo safeguarding and child protection training, including online safety, at induction and at regular intervals.
- Ensuring that there are appropriate filtering and monitoring systems in place.

- Ensuring that the effectiveness of filtering and monitoring systems is reviewed at least annually in liaison with ICT staff and service providers.
- Ensuring that teachers have an awareness and understanding of the filtering and monitoring provisions in place, and manage them effectively and know how to escalate concerns when identified.
- Ensuring that all relevant policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.
- Ensuring compliance with the DfE's 'Meeting digital and technology standards in schools and colleges', with particular regard to the filtering and monitoring standards in relation to safeguarding.
- Ensuring that online safety is a running and interrelated theme throughout Bespoke Learning Ltd.'s policies and procedures.
- Ensuring teachers receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Organising engagement with parents to keep them up-to-date with current online safety issues and how the Bespoke Learning Ltd. is keeping pupils safe.
- Performing the duty of digital lead in line with the Cyber-security Policy.

The DSL will be responsible for:

- Taking the lead responsibility for online safety for Bespoke Learning Ltd.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.
- Ensuring online safety is recognised as part of Bespoke Learning Ltd.'s safeguarding responsibilities.
- Ensuring safeguarding is considered in the Bespoke Learning Ltd.'s approach to remote learning.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and teachers.
- Providing specialist knowledge in relation to filtering system management, e.g. the content and websites pupils should and should not be able to access.

- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.
- Monitoring online safety incidents to identify trends and any gaps in Bespoke Learning Ltd.'s provision, and using this data to update procedures.

All teachers will be responsible for:

- Taking responsibility for the security of ICT systems and electronic data they use or have access to.
- Modelling good online behaviours.
- Maintaining a professional level of conduct in their personal use of technology.
- Having an awareness of online safety issues.
- Ensuring they are familiar with, and understand, the indicators that pupils may be unsafe online.
- Reporting concerns in line with Bespoke Learning Ltd.'s reporting procedure.

Pupils will be responsible for:

- Adhering to the Acceptable Use Agreement and other relevant policies.
- Seeking help from their teacher if they are concerned about something they or a peer have experienced online.
- Reporting online safety incidents and concerns in line with the procedures within this policy.

3. Managing online safety

Teachers will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people, particularly owing to the rise of social media and the increased prevalence of children using the internet.

The DSL has overall responsibility for the school's approach to online safety, with support from deputies and the headteacher where appropriate, and will ensure that there are strong processes in place to handle any concerns about pupils' safety online. The DSL should liaise with

the police or children's social care services for support responding to harmful online sexual behaviour.

Handling online safety concerns

Any disclosures made by pupils to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Child Protection and Safeguarding Policy.

Staff will be aware that harmful online sexual behaviour can progress on a continuum, and appropriate and early intervention can prevent abusive behaviour in the future. Staff will also acknowledge that pupils displaying this type of behaviour are often victims of abuse themselves and should be suitably supported.

The victim of online harmful sexual behaviour may ask for no one to be told about the abuse. The DSL will consider whether sharing details of the abuse would put the victim in a more harmful position, or whether it is necessary in order to protect them from further harm. Ultimately the DSL will balance the victim's wishes against their duty to protect the victim and other young people. The DSL and other appropriate staff members will meet with the victim's parents to discuss the safeguarding measures that are being put in place to support their child and how the report will progress.

Confidentiality will not be promised, and information may be still shared lawfully, for example, if the DSL decides that there is a legal basis under UK GDPR such as the public task basis whereby it is in the public interest to share the information. If the decision is made to report abuse to children's social care or the police against the victim's wishes, this must be handled extremely carefully – the reasons for sharing the information should be explained to the victim and appropriate specialised support should be offered.

Concerns regarding a staff member's online behaviour are reported to Dawn Griffiths, Director of Bespoke Learning Ltd., who decides on the best course of action in line with the relevant policies. If the concern is about Dawn Griffiths, then the relevant LADO should be contacted.

- **BCP** LADO, Allyson Donovan, Hayley Cowmeadow and Tina Cooper
 - on 01202 817600
 - or email LADO@bcp council.gov.uk
- **Dorset** LADO on 01305 221122
 - or email LADO@ddorsetcouncil.gov.uk

[Allegations Against Staff - BCP Safeguarding Children Partnership and the Dorset Safeguarding Children Partnership](#)

Concerns regarding a pupil's online behaviour are reported to the DSL, who investigates concerns and manages concerns in accordance with relevant policies depending on their nature, e.g. the Behaviour Policy and Child Protection and Safeguarding Policy.

Where there is a concern that illegal activity has taken place, Dawn Griffiths will contact the police.

Bespoke Learning Ltd. avoids unnecessarily criminalising pupils, e.g. calling the police, where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity, e.g. a pupil has taken and distributed indecent imagery of themselves. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Child Protection and Safeguarding Policy.

All online safety incidents and the school's response are recorded by the DSL.

4. Cyberbullying

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

- Threatening, intimidating or upsetting text messages
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name
- Unpleasant messages sent via instant messaging
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook
- Abuse between young people in intimate relationships online i.e. teenage relationship abuse
- Discriminatory bullying online i.e. homophobia, racism, misogyny/misandry.

Bespoke Learning Ltd. will be aware that certain pupils can be more at risk of abuse and/or bullying online, such as LGBTQ+ pupils and pupils with SEND.

Cyberbullying against teachers 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.

5. Child-on-child sexual abuse and harassment

Pupils 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, off and online, and will remain aware that pupils are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

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

- Threatening, facilitating or encouraging sexual violence
- Upskirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks
- Sexualised online bullying, e.g. sexual jokes or taunts
- Unwanted and unsolicited sexual comments and messages
- Consensual or non-consensual sharing of sexualised imagery
- Abuse between young people in intimate relationships online, i.e. teenage relationship abuse

Teachers 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. Teachers will be aware that allowing such behaviour could lead to a culture that normalises abuse and leads to pupils becoming less likely to report such conduct.

Teachers will be aware that creating, possessing, and distributing indecent imagery of other 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.

Bespoke Learning Ltd. 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 pupils taking "sides", often leading to repeat harassment. The school will respond to these incidents in line with the Child-on-child Abuse Policy.

6. Grooming and exploitation

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.

Teachers will be aware that grooming often takes place online and that pupils who are being groomed are commonly unlikely to report this behaviour for many reasons, e.g. the pupil may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.

Due to the fact pupils are less likely to report grooming than other online offences, it is particularly important that teachers 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:

- Being secretive about how they are spending their time online.
- Having an older boyfriend or girlfriend, usually one that does not attend the school and whom their close friends have not met.
- Having money or new possessions, e.g. clothes and technological devices, that they cannot or will not explain.

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

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 pupil may be groomed online to become involved in a wider network of exploitation, e.g. the production of child pornography or forced child prostitution and sexual trafficking.

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

Where teachers have any concerns about pupils 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 and Safeguarding Policy.

Radicalisation

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.

Teachers will be aware of the factors which can place certain pupils at increased vulnerability to radicalisation, as outlined in the Prevent Duty Policy. Staff will be expected to exercise vigilance towards any pupils displaying indicators that they have been, or are being, radicalised.

Where teachers have a concern about a pupil relating to radicalisation, they will report this to the DSL without delay, who will handle the situation in line with the Prevent Duty Policy.

7. Mental health

Staff will be aware that online activity both in and outside of AP provision can have a substantial impact on a pupil's mental state, both positively and negatively. The DSL will ensure that training is available to help ensure that teachers understand popular social media sites and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a pupil is suffering from challenges in their mental health. Concerns about the mental health of a pupil will be dealt with in line with the Social, Emotional and Mental Health (SEMH) Policy.

8. Online hoaxes and harmful online challenges

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.

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 pupil and the way in which they are depicted in the video.

Where teachers suspect there may be a harmful online challenge or online hoax towards a pupil they are teaching, they will report this to the DSL immediately.

The DSL will conduct an assessment for any harmful online content brought to their attention, establishing the scale and nature of the possible risk to the pupil, and whether the risk is one that is localised to the pupil or the local area, or whether it extends more widely across the country. Where the harmful content is prevalent mainly in the local area, the DSL will consult with the LA about whether quick local action can prevent the hoax or challenge from spreading more widely.

Prior to deciding how to respond to a harmful online challenge or hoax, the DSL may contact the LADO to decide whether each proposed response is:

- In line with any advice received from a known, reliable source, e.g. the UK Safer Internet Centre, when fact-checking the risk of online challenges or hoaxes.
- Careful to avoid needlessly scaring or distressing pupils.
- Not inadvertently encouraging pupils to view the hoax or challenge where they would not have otherwise come across it, e.g. where content is explained to younger pupils but is almost exclusively being shared amongst older pupils.
- Proportional to the actual or perceived risk.
- Helpful to the pupils who are, or are perceived to be, at risk.
- Appropriate for the relevant pupils' age and developmental stage.
- Supportive.
- In line with the Child Protection and Safeguarding Policy.

Where the DSL's assessment finds an online challenge to be putting a pupil at risk of harm, they will ensure that the challenge is directly addressed to the relevant pupil.

9. Cyber-crime

Cyber-crime is criminal activity committed using computers and/or the internet. There are two key categories of cyber-crime:

- **Cyber-enabled** – these crimes can be carried out offline; however, are made easier and can be conducted at higher scales and speeds online, e.g. fraud, purchasing and selling of illegal drugs, and sexual abuse and exploitation.
- **Cyber-dependent** – these crimes can only be carried out online or by using a computer, e.g. making, supplying or obtaining malware, illegal hacking, and ‘booting’, which means overwhelming a network, computer or website with internet traffic to render it unavailable.

Bespoke Learning Ltd. will factor into its approach to online safety the risk that a young person with a particular affinity or skill in technology may become involved, whether deliberately or inadvertently, in cyber-crime. Where there are any concerns about a pupil’s use of technology and their intentions with regard to using their skill and affinity towards it, the DSL will consider a referral to the Cyber Choices programme, which aims to intervene where children are at risk of committing cyber-crime and divert them to a more positive use of their skills and interests.

The DSL will ensure that pupils are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully.

10. Online safety training for staff

The DSL will ensure that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation, and understanding the expectations, roles and responsibilities relating to filtering and monitoring systems. All staff will be made aware that pupils are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life.

Teacher training will include a specific focus on harmful online narratives such as misinformation, disinformation, and conspiracy theories, helping staff to recognise the signs of influence or vulnerability among pupils.

Training will equip teachers with the knowledge and confidence to identify signs of online harm, respond appropriately to disclosures or concerns, and support pupils in developing critical thinking skills and safe online behaviours.

Teachers will also be guided on how to embed online safety themes across the AP curriculum. promoting digital safeguarding.

Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using.

The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

- How to evaluate what they see online
- How to recognise techniques used for persuasion
- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support
- Knowledge and behaviours that are covered in the government's online media literacy strategy

The online risks pupils may face online will always be considered when developing the curriculum.

Bespoke Learning Ltd.'s approach to teaching online safety in the curriculum will reflect the ever-evolving nature of online risks, ensuring pupils develop the knowledge and resilience to navigate digital spaces safely and responsibly. Online safety education will address four key categories of risk: content, contact, conduct, and commerce.

Content Risks

Pupils will be taught how to critically evaluate online content and identify material that is illegal, inappropriate, or harmful. The curriculum will include discussions around harmful content such as pornography, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, misinformation, disinformation (including fake news), and conspiracy theories. Lessons will equip pupils with the skills to question sources, verify information, and understand the dangers of engaging with such content.

Contact Risks

Bespoke Learning Ltd. will educate pupils about the potential dangers of interacting with others online. Pupils will explore topics such as peer pressure, commercial exploitation, and grooming tactics used by adults who pose as children or young adults. They will learn how to recognise unsafe interactions, use privacy settings effectively, and report any concerning behaviour or messages to trusted adults and platforms.

Conduct Risks

Pupils will be guided on how their own online behaviour can impact both themselves and others. The curriculum will address the risks associated with creating, sharing, or receiving explicit images, including both consensual and non-consensual exchanges of nudes and semi-nudes. Online bullying, including the use of social media and messaging platforms to harass or intimidate others, will also be a key focus. Pupils will be taught responsible digital conduct and the legal and emotional consequences of harmful behaviour.

Commerce Risks

The curriculum will also include education on online commercial risks. Pupils will be informed about the dangers of online gambling, exposure to inappropriate advertising, and financial scams such as phishing. They will learn how to recognise fraudulent schemes, protect their personal and financial information, and seek help when confronted with suspicious online activity.

The DSL will develop Bespoke Learning Ltd.'s online safety curriculum. Pupils will be consulted on the online safety curriculum, where appropriate, due to their unique knowledge of the kinds of websites they and their peers frequent and the kinds of behaviours in which they engage online.

Before conducting a lesson or activity on online safety, the teacher will consider the topic that is being covered and the potential that their pupil may have suffered or may be suffering from online abuse or harm in this way. The DSL will advise the teacher on how to best support any pupil who may be especially impacted by a lesson or activity. Lessons and activities will be planned carefully so they do not draw attention to a pupil who is being or has been abused or harmed online, to avoid publicising the abuse.

During an online safety lesson or activity, the class teacher will ensure a safe environment is maintained in which the pupil feels comfortable to say what they feel and ask questions, and are not worried about getting into trouble or being judged.

If a teacher is concerned about anything a pupil raises during online safety lessons and activities, they will make a report in line with the Child Protection and Safeguarding Policy.

If a pupil makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member will follow the reporting procedure outlined in the Child Protection and Safeguarding Policy.

11. Use of technology in the classroom

The technology which may be used during lessons, including the following:

- Laptop
- Email

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that pupils use these platforms at home, the class teacher will review and evaluate the resource. Teachers will ensure that any internet-derived materials are used in line with copyright law.

Pupils will be supervised when using online materials during lesson time – this supervision is suitable to their age and ability.

12. Use of smart technology

While Bespoke Learning Ltd. recognises that the use of smart technology can have educational benefits, there are also a variety of associated risks. Pupils will not use smart technology in lessons with Bespoke Learning Ltd. However, pupils will be educated on the appropriate use of personal devices for their safety.

Pupils will be taught that inappropriate uses of smart technology may include:

- Using mobile and smart technology to sexually harass, bully, troll or intimidate peers.
- Sharing indecent images, both consensually and non-consensually.
- Viewing and sharing pornography and other harmful content.

Pupils will not be permitted to use smart devices or any other personal technology whilst in the classroom with Bespoke Learning Ltd.

Bespoke Learning Ltd will endeavour to ensure that it keeps up to date with the latest devices, platforms, apps, trends and related threats.

Bespoke Learning Ltd. will consider the 4Cs (content, contact, conduct and commerce) when educating pupils about the risks involved with the inappropriate use of smart technology. Educating parents

Parents will be made aware of the various ways in which their children may be at risk online, including, but not limited to:

- Child sexual abuse, including grooming.
- Exposure to radicalising content.

- Sharing of indecent imagery of pupils, e.g. sexting.
- Cyberbullying.
- Exposure to age-inappropriate content, e.g. pornography.
- Exposure to harmful content, e.g. content that encourages self-destructive behaviour.

Parents will be informed, the teacher, of the ways in which they can prevent their child from accessing harmful content at home, e.g. by implementing parental controls to block age-inappropriate content.

13. Filtering and monitoring online activity

Bespoke Learning Ltd. uses public computers in BCP and Dorset libraries. The libraries have appropriate filters and monitoring systems in place which meet the DfE's '[Filtering and monitoring standards for schools and colleges](#)'.

- **Filtering:**

This involves software that identifies and blocks access to specific types of websites or online content deemed harmful or inappropriate.

- **Monitoring:**

This involves recording user activity, such as the websites visited and the search terms used, to identify potential misuse of the library's internet services.

14. Emails

Pupils do not have a Bespoke Learning Ltd. email address.

15. Generative artificial intelligence (AI)

Pupils will only be permitted to use generative AI in lessons with close supervision by their teacher.

For any use of AI, Bespoke Learning Ltd. will:

- Comply with age restrictions set by AI tools and open access large language models (LLMs).

- Consult KCSIE to ensure all statutory safeguarding obligations and AI tools are used safely and appropriately.
- Refer to the DfE's [generative AI product safety expectations](#) and [filtering and monitoring standards](#).

Bespoke Learning Ltd. will take steps to prepare pupils for changing and emerging technologies, e.g. generative AI and how to use them safely and appropriately with consideration given to pupils' age.

Bespoke Learning Ltd. will ensure that pupils are not accessing or creating harmful or inappropriate content, including through generative AI.

Bespoke Learning Ltd. will take steps to ensure that personal and sensitive data is not entered into generative AI tools and that it is not identifiable.

Bespoke Learning Ltd. will make use of any guidance and support that enables it to have a safe, secure and reliable foundation in place before using more powerful technology such as generative AI.

16. Social networking

There is no use of social media by teachers or pupils at Bespoke Learning Ltd.

17. The Bespoke Learning Ltd. website

Dawn Griffiths, Director, is responsible for the overall content of Bespoke Learning Ltd.'s website – she will ensure the content is appropriate, accurate, up-to-date and meets government requirements.

18. Remote learning

All remote learning will be delivered in line with the school's Remote Education Policy. This policy specifically sets out how online safety will be considered when delivering remote education.

19. Monitoring and review

The next scheduled review date for this policy is 07.09.2026.

Any changes made to this policy are communicated to all teachers working on behalf of Bespoke Learning Ltd.

This policy was created on 01.09.26 and will be reviewed annually by Dawn Griffiths, Director, Bespoke Learning Ltd.

Review	Amendments