Online Safety Policy

Date	October 2026
Approved By	Headteacher
Date Approved	October 2026
Review Date	October 2027
Staff role responsible for review	Deputy Headteacher

This policy applies to all stakeholders within Ivel Valley School & College

Introduction

Ivel Valley has good, strong processes in place to ensure the online safety of all our community. We know that technology enables us to do lots of amazing things - communicate, learn new skills, develop existing skills and share information - but we also know that working online comes with a number of risks, and that the nature of these risks is constantly evolving and changing. Our staff surveys reflect that our staff feel confident that we teach children and young people how to be safe online at Ivel Valley, but we know that we need to work to continually educate our whole school and college community to use technology in a safe and empowering way.

The purpose of this policy

This policy aims to clarify the risks of online safety and the proactive measures that we take to keep ourselves safe online. If we have concerns about anything to do with online safety, we want pupils and staff to know how to identify, intervene and escalate these concerns in a clear, supportive and appropriate way.

Every pupil at Ivel Valley has an Education, Health and Care Plan (EHCP), so we know that they need sensitive, specialised support in all areas, including online safety. This policy reflects this need.

What are the risks?

Our approach to online safety is based on addressing the following categories of risk, as per the current version of Keeping Children Safe in Education:

- **content**: being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, extreme sexual of physical violence, misinformation, disinformation (including fake news) and conspiracy theories
- **contact**: being subjected to harmful online interaction with other users or generative AI applications that simulate this; for example: 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**: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images, including those generated using AI and online bullying,
- **commerce**: risks such as online gambling, inappropriate advertising, phishing or financial scams

How do we keep ourselves safe online at Ivel Valley?

- We encourage staff and pupils to have ongoing conversations about internet use, recognising that openly talking about with children and young people about what they do online is the best way to understand their experiences and feelings about being online.

- Staff give pupils lots of opportunities to engage with technology in positive ways, including use of iPads, laptops, interactive white boards, switches, BeeBots, VR headsets and digital cameras. We are always looking for exciting augmentative ways to access and use technology to enhance our learning.

- At Ivel Valley, all pupils follow our purpose-written Ivel Valley curriculum. Online safety is fully integrated into our curriculum; it is built into our 'understanding the world' and 'PSED' areas of learning strands, with clear curriculum guidance documents to aid teachers, and is augmented by a computing curriculum. We often discuss the importance of teaching online safety for all ages and at all levels of learning, to help

staff understand what this might look like for their pupils' specific needs – see for example the document in Appendix One. A large number of supportive resources to aid teaching and learning are saved in our shared 'Curriculum' drive. Teachers are expected to deliver a minimum of two online safety lessons per half term – this is likely to need to increase as pupils become more independent and explorative users of the internet. The content of these will be based on individual need, individual stages on the curriculum and the topic breadth grid. At least one observation related to online safety should be recorded per pupil per half term on Evidence for Learning, using the 'online safety' tag. Where appropriate, pupils in Key Stage 3 and above are given increasing opportunities to use a device to complete their classwork, and some of them have use of their own Ivel Valley email addresses, to help to maintain positive contact with each other and staff whilst using a safe system. Staff must recognise that at these ages pupils are increasingly likely to use their own devices and have their own social media accounts, although it is notable that a social media ban for under-16s is due to be implemented in spring 2027. It is vital that staff take time to discuss with pupils how they access the internet and continually offer teaching that is responsive to individual pupil need.

- We recognise that due to our pupils all having individual additional needs, they will all access technology and the internet in unique ways, and that their learning connected to online safety might not progress in a linear way. It is important that teachers have the flexibility to understand and respond to individual pupil need regarding online safety, in correspondence with their identified strengths and needs, considering the risks highlighted above and with reference to the curriculum.

- We have a pupil Online Safety group led by our Technology and Online Safety Lead, to help staff better understand how pupils are using the internet.

- We ensure that we are compliant with the Department for Education's filtering and monitoring standards. Our DSL and IT team work together to ensure that all appropriate safety settings and filtering arrangements are applied to all devices that are used around the school and college, including laptops and iPads, and the 'Bring your own device' Wifi. This provision has an annual strategic review, and ongoing operational checks. We use a highly reputable provider for wifi and filtering. Our filtering successfully blocks child sexual abuse content, terrorism content, adult content and offensive language. If any staff or pupils try to search for any blocked content or access a website of concern, a notification is sent to the Designated Safeguarding Lead (DSL) and Network Manager, to allow them to consider whether any further action is necessary.

- We use reputable, secure systems to communicate with our wider community, including our Ivel Valley email addresses, Bromcom, MyChildAtSchool and Class Dojo.

- Staff watch NCSC (National Cyber Security entre) Cyber security training for school staff as part of their induction process.

Generative Artificial Intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. We understand the valuable potential that generative AI holds for schools. For example, it can be used to enhance pedagogical methods, customise learning experiences and progress educational innovation. However, there are also numerous risks posed by AI, including data protection breaches, copyright issues, ethical complications, safeguarding and compliance with wider legal obligations. AI tools are only as accurate as the information they're trained on. They may generate responses that are incorrect, biased, or inappropriate.

The two key principles that all staff must abide by are:

- no one is permitted to enter identifying, personal or sensitive data into unauthorised generative AI tools

or chatbots. If personal and/or sensitive data is entered into an unauthorised generative AI tool, we will treat this as a data breach and will follow the personal data breach procedure outlined in our data protection policy.

- Staff might use AI tools as a starting point for generating content (such as lesson plans, policies or risk assessments), but must always check and adapt the results so they are:
    - Taking the best interests of staff, pupils and the school/trust into account
    - In line with our policies, procedures and guidelines
    - Checked for factuality and sense

AI technology, and the benefits, risks and harms related to it, evolves and changes rapidly. We have provided training for teachers on safe and appropriate use of generative AI, but this need to be an ongoing conversation. We have an AI policy to provide guidance on what safe and appropriate use of AI looks like at Ivel Valley.

Other specific areas of online safety

Acceptable internet use

- Staff are all expected to sign an agreement regarding appropriate use of IT and the internet and must comply with this. This is signed as part of induction and then every September.
- Pupils and students from KS3 upwards are expected to sign an accessible agreement regarding using the internet, if appropriate considering their level of cognition (see Appendix Two). Students at the college are allowed to keep their mobile phones on them during the day, and they must sign an acceptable use agreement regarding this.
- Visitors will be expected to read and agree to our terms on acceptable use of IT, if relevant.
- Use of Ivel Valley's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.
- The filtering arrangements described above enable monitoring of the websites visited by all of those using the internet at Ivel Valley to ensure they comply with our acceptable internet use requirements.

Cyberbullying or online abuse

- Children can abuse their peers online through:
    - Abusive, harassing, and misogynistic or misandrist messages
    - ~~Non-consensual sharing of~~ ~~indecent~~ Making or sharing nude and semi-nude images and/or videos, especially around chat groups. This includes AI-generated images.
    - Sharing of abusive images and pornography
- Staff work to help pupils to understand that bullying and abuse can happen online as well as in real life, to understand how this might look.
- Staff encourage pupils to understand and have strategies of how to respond and then report any concerns, whether they relate to themselves or others.
- Online abuse is covered in initial safeguarding training and is constantly reflected on through weekly safeguarding update emails.
- Any safeguarding concerns must be reported to the safeguarding team and using CPOMS, as per the safeguarding and child protection policy.
- If illegal, inappropriate or harmful material has been spread among pupils, we will use all reasonable endeavours to ensure the incident is contained. The DSL will consider whether the incident should be

reported to the police if it involves illegal material and will work with external services if it is deemed necessary to do so.

- All incidents regarding the making or sharing of nude or semi-nude images, including AI-generated images, will trigger safeguarding processes.
- The safeguarding policy contains specific guidance around youth produced sexual imagery.
- The anti-bullying policy also considers cyber-bullying.

Examining electronic devices

- Education staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so. 'Good reasons' could be that the image or file could cause harm, disrupt teaching, or breach school rules.
- Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

Personal devices and mobile phones

- Ivel Valley School is mobile phone-free by default.
- Some pupils bring personal devices into school to use whilst on their journey to / from school. This is acceptable, but families must be aware that Ivel Valley cannot be responsible for ensuring the safety of these devices. Pupils cannot keep these devices on them during the school day. Pupils are supported to keep personal devices in a safe place throughout the day, for example in a classroom safe or in the main office.
- The exception is when there is a specific need for pupils to use devices as a learning tool, for example as a communication aid. Specifics around this use should be discussed between home and school and recorded.
- College students are allowed to bring their phones to college with them; staff work with students to teach them how to use their phones to aid their independence, for example using calculators, accessing shopping apps, taking images as aide memoirs, following QR codes, or calling for help when travelling independently. Students can use their phones during break times. This must happen in the context of proactive safety messages from staff. Students must sign a mobile phone use agreement. They can access a 'Bring your own device' wifi, which offers high levels of filtering and monitoring.

Roles and responsibilities

All staff will:

- be aware that children are at risk of online abuse; that technology is a significant component in many safeguarding and wellbeing issues; and that in many cases, abuse and other risks will take place concurrently both online and offline
- support and encourage pupils to engage positively with technology and internet access
- supervise and monitor pupils whilst they access the internet, with an awareness that pupils might access inappropriate or harmful material deliberately or accidentally
- ensure that pupils only access the internet via a pupil login, not a staff one (this is due to different levels of filtering)

- report any concerns around online safety, including sending of nude or semi-nude images (including AI-generated images), cyberbullying and sexual violence or harassment, using CPOMS, as per the safeguarding policy
- adhere to relevant policies and training alongside this policy, such as GDPR, Prevent, code of conduct, data protection, confidentiality and use of IT agreement
- be aware that if they misuse IT, they may be subject to disciplinary procedures
- not have their mobile phones on their person whilst they are in contact with pupils, unless for one of two reasons:
    - Expecting a personal phone call, such as a GP appointment, with permission from the leadership team
    - When supporting pupils offsite, for safety and contact purposes
- not use 'smart glasses' at any time on school premises, unless agreed with and risk assessed with SLT for accessibility purposes
- never take photos of pupils on their personal devices (mobiles or cameras)
- only use smart watches (e.g. Apple watches) **as watches** around the pupils
- ensure that they use any work devices safely and appropriately, as per the Use of IT agreement, which includes expectations around locking devices
- access GDPR training on joining Ivel Valley, and again yearly, and actively implement this
- share job vacancies on social media if they want to, but apart from this, **no** information about Ivel Valley will be posted on personal social media
- ensure that their social media is either set as private; if public, they must ensure that content is appropriate considering their position of responsibility
- maintain professional boundaries around communicating with pupils online:
    - never communicating with pupils through social media
    - only using the Ivel Valley email system to email pupils
    - only emailing them or responding to their emails during school hours
    - maintaining professional boundaries in emails
- Office-based staff only: complete a yearly Display Screen Equipment self-assessment and follow guidance about how to support good posture.

The Headteacher will:

- ensure that this policy is implemented consistently and effectively throughout Ivel Valley
- ensure that the DSL accesses training to enable a good awareness of online safety
- work with relevant staff to ensure that AI is used safely and effectively.

The Designated Safeguarding Lead (DSL) will:

- take lead responsibility for safeguarding and child protection, including online safety and understanding the filtering and monitoring systems and processes in place
- work with the Network Manager on an annual in-depth review of filtering and monitoring systems
- work with relevant staff to address any online safety issues or incidents, and ensure that they are recorded appropriately on CPOMS
- work with relevant staff to ensure that any safeguarding concerns, including incidents of child-on-child abuse, or sexual violence / harassment are managed in line with the safeguarding & child protection policy
- lead on delivering or organising online safety training for staff, including induction, yearly refreshers, ongoing regular updates, and covering Prevent (dealing with extremism and radicalisation, which predominantly happens online)
- endeavour to be aware of new and emerging online safeguarding threats ~~posed by AI~~, and share this information with staff
- share relevant online safety information with parents / carers

- include relevant information about online safety in safeguarding reports to governors
- support the Headteacher in ensuring that this policy is implemented consistently and effectively throughout Ivel Valley.

The Network Manager will:

- work with the senior leadership team to ensure that Ivel Valley is meeting the DfE filtering and monitoring standards
- put in place an appropriate level of security protection procedures that protects children and young people, without unreasonably impacting teaching and learning
- review and update these systems on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at Ivel Valley – including blocking access for pupils and staff to potentially dangerous or extremist sites
- ensure that the Ivel Valley IT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- conduct regular security checks and system monitoring exercises
- work with SLT (predominantly the Business Manager and the DSL) to review Use of ICT / Acceptable Use agreements for all stakeholders
- allocate equipment and track this through an asset register
- work with the IT Apprentice to maintain the disaster recovery plan and ensure that it is responsive to evolving challenges
- liaise with the DSL or Headteacher regarding any concerns that they identify in connection with online safety or cyberbullying.

The Technology & Online Safety Lead will:

- support the leadership team in ensuring that appropriate learning is implemented that gives pupils sufficient knowledge and skills to stay safe online
- support the leadership team in monitoring and evaluating the impact of the teaching and learning of online safety throughout Ivel Valley
- arrange expert input from external professionals where required
- work with the Curriculum Lead to review and develop the IT curriculum
- support the DSL in raising parent/carer awareness
- support teachers to access appropriate and exciting ways of teaching online safety, by promoting resources and developing teachers' knowledge.

Governors will:

- ensure that they have a full understanding of this policy and that the school keeps pupils safe online
- hold relevant staff to account for implementing it effectively.

Pupils will:

- engage in learning activities about online safety, adapted to their individual needs
- where appropriate, understand that their internet activity is monitored
- follow the Golden Rules or Expect Respect rules whilst engaging with others on the internet
- look after the technology that they use
- use technology in a safe and appropriate way.

Our accessible online safety policies for sharing these expectations with pupils can be found in Appendix Three.

Families will:

- share with us any important or relevant information about how their child accesses technology and the internet
- make us aware of any concerns about their child's online safety, to enable us to respond appropriately from a school or college perspective
- engage with updates on Dojo that are relevant to them
- contact our Network Manager if help is needed to set filters
- take reasonable steps to ensure that their child doesn't access inappropriate content.

Legal framework & statutory guidance

Linked national guidance:

- Cyber bullying: advice for headteachers and school staff (DfE, November 2014)
- Filtering and monitoring standards for schools and colleges (DfE, current version)
- Data (Use and Access) Act 2025
- Keeping Children Safe in Education (DfE, current version)
- Prevent duty guidance (DfE, 2023)
- Preventing and tackling bullying (DfE, July 2017)
- Relationships Education, Relationships and Sex Education (RSE) and Health Education (DfE, current version)
- Searching, screening and confiscation: advice for schools (DfE, July 2022)
- Teaching online safety in schools (DfE, January 2023)

Linked policies:

- Anti-Bullying policy
- Code of conduct
- Confidentiality policy
- Data protection and use of IT agreement
- Data protection policy
- Safeguarding & child protection policy
- Use of Artificial Intelligence (AI) policy

Equalities & inclusion

Research shows that vulnerable children experience significant benefits from being online. However, they are also more likely to experience online risks. As such, they require very specific support to develop digital resilience to benefit safely. Ivel Valley strives to ensure that children and young people all have meaningful access to technology, in a way that accommodates their individual special needs. It is important that online safety teaching is delivered in ways that acknowledge these needs and makes online safety accessible for pupils working at all levels.

AI tools can perpetuate existing biases, particularly towards protected characteristics including sex, race and disability. For this reason, critical thought must be applied to all outputs of authorised AI applications. This means fact and sense-checking the output.

Safeguarding implications

Technology is a significant component in many safeguarding and wellbeing issues, and we must be mindful that all children are at risk of online abuse. This policy is additional to the Safeguarding and Child Protection policy; any safeguarding concerns raised in connection with online safety should be managed according to the Safeguarding and Child Protection policy.

Sustainability implications

We recognise that our use of digital technology and online resources has environmental impacts. Steps we take to improve sustainability are:

- Responsible use of technology is promoted: staff and pupils are encouraged to use digital devices efficiently, switch off equipment when not in use, and utilise energy-saving settings
- We encourage staff to review and delete unnecessary files and emails, use cloud storage responsibly, and ensure personal data is disposed of securely and sustainably
- Where possible, we attempt to maintain devices to extend their lifespan. When no longer needed, they are recycled or disposed of following best environmental and data security practices
- Where possible, we purchase energy-efficient equipment and consider the environmental impact of digital resource choices.

Appendices

- **ONE:** Online safety at early stages of learning
- **TWO:** Pupil acceptable use agreement
- **THREE:** Accessible policies for pupils
- **FOUR:** Online safety risk assessment
- **FIVE**: Prevent specific risk assessment

APPENDIX ONE: online safety at early stages of learning

Online safety at early stages of learning

Children need to learn online safety at all ages, and all stages of learning. Online safety does not just apply to older pupils who use the internet independently; lots of children at early stages of learning use the internet to watch cartoons, films and songs.

The four areas of risk in online safety are identified as content, contact, conduct and commerce. There is more about these in our online safety policy. They still apply to pupils at early stages of learning, just in different ways!

Here are some top tips for what online safety work can look like at early stages of learning:

CONTENT

- Explore fun and safe activities on the internet together, choosing apps and games that allow them to develop skills.
- Model what you do if you see something that you don't like.

CONTACT

- Model kindness online, saying kind words and sending kind messages to others.
- Model consent and respectful sharing practice, for example asking to take photos of them, even if you think they aren't listening to you!

CONDUCT

- Work on cause-and-effect games, such as apps where you tap the screen to make fireworks explode. This enables them to build an understanding that they can influence what they see on a screen – it doesn't have to happen to them.
- Describe what you are thinking and doing, and if appropriate, ask questions, such as "I wonder what will happen when we tap here?"
- Practise turn taking on the internet.
- Access simple stories and videos about online safety – there are lots on YouTube, and lots are signposted in the Curriculum Resources folder on the shared drive.
- Teach them to ask for help when something isn't working how they want it to on a device.

COMMERCE

- It's important to ensure that appropriate safety settings and filters are on all devices used by pupils. Younger pupils have sometimes share things or make purchases inadvertently! They must always be supervised when using technology.

APPENDIX TWO: pupil acceptable use agreement

Using the Internet at Ivel Valley

I understand that:

- The internet can help us in amazing ways, but we must follow some rules to stay safe.
- Staff are there to help me learn how to use the internet safely.
- Not everything that I see on the internet is true.
- Emily and Neil make sure that people are using the internet safely, so they will see if I try to do something inappropriate on the internet at Ivel Valley.
- If I break these rules, I might not be able to use the internet at Ivel Valley.

I know that I must:

- Listen to what staff say and only use websites or apps that they have agreed to me using.
- Ask for help if I think I have made a mistake online.
- Ask for help if I see something online that I don't like.
- Be kind online: bullying, being mean and bad language is not ok on the internet.
- Not share private information about myself online.
- Not share private information or pictures about anyone else without their consent.
- Not speak to anyone online that I don't know whilst I am online at Ivel Valley.
- Not share information about Ivel Valley online unless staff have said it's ok.
- Not try to buy anything whilst I am online at Ivel Valley.
- Keep my username and password private and safe.
- Take care of all our IT equipment, like laptops and iPads.

I agree to these rules.

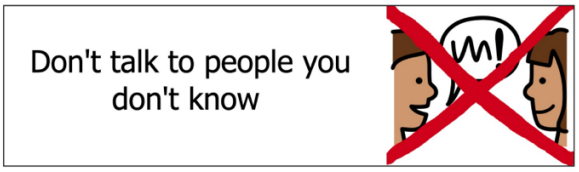
Signed:

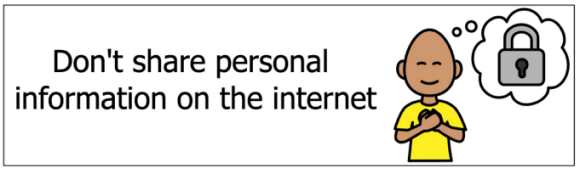
Date:

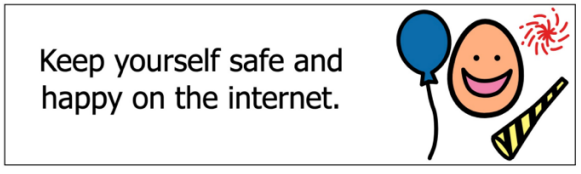
APPENDIX THREE: accessible policies for pupils

Online safety at Ivel Valley

	Online safety means keeping you safe and happy when you use the internet.
	There are lots of brilliant things about using the internet, like playing games, finding information and talking to friends.
	We might see things online that we don't like, or might be illegal. We must tell someone if this happens.
	People online might see mean things, or try to make us do things that aren't safe. We must tell someone if this happens.
	We need to know what information about ourselves we should or shouldn't share online.
	Some information online is 'fake news', or is a scam. We need to understand what this means.
	We have to take care of the technology that we use.
	At school and college, adults have to make sure that everyone is using the internet safely.







APPENDIX FOUR: online safety risk assessment

Description	Details	Who?	Mitigating action
Exposure to inappropriate online content	• Commercial – adverts, spam, sponsorship, personal info • Extremist - violent / hateful content • Sexual - pornographic or unwelcome sexual content • Values – bias, racist, misleading info or advice	Children & staff	• Use of IT Agreement • Appropriate filtering • Pupils actively taught how to report concerns about content • Information shared with parents/carers about filtering systems at home • All staff have Prevent training
Inappropriate online contact	• Aggressive - being bullied, harassed or stalked • Sexual – harassment, meeting strangers, being groomed • Values – self harm, unwelcome persuasions NOTE: Ivel Valley pupils may be particularly vulnerable to this due to their SEND	Children & staff	• Online Safety policy • Reporting mechanisms • A culture where pupils are supported to share worries safely • Appropriate monitoring • Online safety teaching & learning • Work to identify SEND-specific resources
Inappropriate online behaviour	• Commercial – Illegal downloading, hacking, gambling, financial scams, terrorism • Aggressive - being bullied, or harassing others • Sexual – peer harassment, creating and uploading inappropriate material • Values – providing misleading info or advice	Children & staff	• Use of IT Agreement • Safeguarding policy • AI policy • Infrastructure security • Appropriate monitoring • Online safety teaching & learning • Work to identify SEND-specific resources • Work with families to agree appropriate supports
Cyber and Information Security	• Data Protection – data loss or compromised • Security Intrusion – information or access is compromised e.g. hack or virus/malware	Staff	• GDPR Policy • GDPR training (including advice on passwords) • AI policy

			• Data Protection Officer • Firewall security • Protective systems (anti- virus) • Software updating regime • Incident management • Guidance for staff on safe use of AI • Staff access NCSC Cyber security training at induction
Safeguarding	• Staff capability to recognise, respond and resolve issues	Staff	• Training programme including induction, refreshers and weekly safeguarding updates • Use of CPOMS to record information • Senior leadership and Designated Safeguarding Lead responsibilities • Clear lines of escalation • Staff survey to track staff confidence

APPENDIX FIVE: Prevent specific risk assessment

Description	Yes / No	Who?	Supporting action
Does your safeguarding policy make explicit that the school sees protection from radicalisation and extremist narratives as a safeguarding issue?	Yes	DSL	Radicalisation and Prevent is identified in the safeguarding policy, and Keeping Children Safe in Education is referred to for further detail.
Are the lead contact for Prevent responsibilities clearly identified in the policy?	Yes	DSL	Having such a large staff team, we are consistent in guiding staff to refer all safeguarding concerns to the DSL or deputy. They are the lead contacts for Prevent.
Does the policy make explicit how Prevent concerns should be reported within school?	Yes	DSL	We give our staff clear information to report all concerns through CPOMS, which ensures consistency. The DSL remains up-to-date with Central Bedfordshire reporting procedures. More detail can be found in the safeguarding policy. The DSL and deputies know that
Are staff aware of relevant local and national risks?	Yes	DSL	The threat to the UK from all forms of terrorism is ranked as SEVERE. Most Prevent referrals in the local area are connected to a mixed / unclear / unstable profile. Information regarding this is shared with staff during annual refreshers and ongoing email updates. The DSL receives Prevent-specific updates from the local Prevent in Education Officer. There is ongoing work with local partners. Staff are updated using weekly safeguarding update emails. Our Technology and Online Safety Lead supports with ongoing curriculum review to ensure that we are constantly responding to risks as appropriate.
Do staff share information with relevant partners in a timely manner?	Yes	DSL	The DSL and deputy DSL have worked with the Prevent team and made referrals when appropriate, seeking guidance for complex cases.
Are Fundamental British Values (FBV) considered in curriculum planning?	Yes	SLT	Our curriculum was designed in-house, and FBVs were integrated into the development process. The Curriculum Lead continues to demonstrate a commitment to FBV in ongoing review processes. The curriculum is broad and balanced. Personal, Social & Emotional Development is one of our prime areas of learning; Understanding the World is one of our specific areas.

			Diversity has been a significant area of focus and development. We have worked to explicitly identify diverse role models and resources alongside different topics.
Thinking about an incident of radicalisation and/or extremism - has the setting considered specific potential areas of risk?	Yes	SLT	We have a School Emergency Plan on a shared 'emergencies' drive that SLT has accessed. We have lockdown procedures in place, which have been practised by pupils and staff. We have experience in managing SARs. We have taken action in readiness of Martyn's Law.
Does the school have clear guidance for visiting speakers?	Yes	SLT	For any external services being sought, we only use known and recommended training providers. When visitors arrive, the office team follows clear procedures to verify their identity. Our premises are currently only used by established local charities that provide disability support, or by groups connected to education, health or social care partners. Safer recruitment checks are carried out on all staff.
Have ALL staff received appropriate training on Prevent?	Yes	DSL	All staff complete DfE Prevent training as part of their induction. This is recorded on the Single Central Record. Prevent is also referred to in initial safeguarding training. Relevant updates are shared throughout the year in safeguarding update emails. Annual refreshers are embedded in safeguarding training, informed by training accessed by the DSL. Staff safeguarding surveys demonstrate a strong confidence in following safeguarding processes, including recognising signs of abuse and vulnerability.
Does the Online Safety policy refer to the requirements of the Prevent guidance?	Yes	DSL	This risk assessment is appended to the online safety policy to firmly connect Prevent strategy with online safety – the online world is prevalent in nearly all Prevent cases. The policy also clearly reflects the need for appropriate filtering that blocks access to dangerous or extremist websites. Filtering and monitoring responsibilities are taken seriously, and the DSL and Network Manager work together to review and monitor these processes. The Technology and Online Safety Lead works with the Bedfordshire Police Cyber Choices officer to deliver preventative work around cybercrime to pupils.
Are protocols are in place to manage the layout, access and use of any space provided for the purposes of prayer, contemplation and faith facilities?	No		There are no relevant facilities at Ivel Valley.
Is there clear guidance on governing the display of	Yes	SLT	There is display guidance for classrooms and this is monitored by the Assistant Headteachers. There is not a

materials internally at the school?			culture of staff displaying their own materials in the staffroom; this is monitored.