ONLINE SAFETY POLICY

Note: 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.

Key members of staff:

 Network Manager - Neil	 Designated Safeguarding Lead – Emily Sidhu	 Understanding the World area of learning lead for KS4&5, technology focus – Aaron Norwood
 Deputy Designated Safeguarding Lead – Roger Williams	 Principal – Joe Creswick	 Business Manager – Hannah Doran

Approved by Principal: May 2022

To be reviewed, yearly: May 2023

Note: Children includes everyone under the age of 18. At Ivel Valley, our young people may stay in our college provision until they are 19 years of age. Due to their vulnerability, this policy will continue to be used until they leave Ivel Valley. When we refer to 'children' and 'school' in this policy, we also cover 'young adults' and 'college'. This policy also applies to pupils in the Early Years Foundation Stages (EYFS).

WE NEED TO BE AWARE OF: WHAT IS THIS POLICY ABOUT?

Ivel Valley has good, strong processes in place to ensure the online safety of all of our school community, especially our pupils and staff. 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 are constantly evolving and changing. We work to continually educate our whole school and college community to use technology in a safe and empowering way. If we have concerns about anything to do with online safety, we want 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.

WE NEED TO BE AWARE OF: WHAT ARE THE RISKS?

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

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

WE NEED TO BE AWARE OF: HOW DO WE KEEP OURSELVES SAFE ONLINE AT IVEL VALLEY?

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

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

- At EY-KS3, online safety is fully integrated into our curriculum; it is built into our 'understanding the world' and 'PSED' areas of learning strands. We often discuss the importance of teaching online safety for all ages. A large number of supportive resources to aid teaching and learning are saved in our shared 'Curriculum' Google Drive. Teachers will be expected to deliver a minimum of two online safety lessons per half term. 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.

- At KS4 and 5, online safety is integrated into ASDAN accreditations, and teachers augment this with an ongoing coverage of online safety . Where appropriate, these pupils are given increasing opportunities to use laptops to complete classwork, and some of them have use of their own Ivel Valley email address, to help to maintain positive contact with each other and staff, 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. 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 all of our pupils 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 National Curriculum computing programmes of study and RSE guidance – see appendix one;

- Our IT team will ensure that all appropriate safety settings and filtering arrangements are applied to all devices that are used around the school, including laptops and iPads.

- We utilise the Schools Broadband Prevent alerting system that notifies the Designated Safeguarding Lead (DSL) if anyone accesses or tries to access a website that falls into a category of concern. This allows the DSL to take appropriate supportive action.

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

WE NEED TO BE AWARE OF: WHAT DO WE EXPECT OUR STAFF TO DO?

All staff will:

- 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;
- be aware that technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse;
- report any concerns around online safety, including sending of nude or semi-nude images, cyberbullying and sexual violence or harassment, using CPOMS, as per the safeguarding policy;
- adhere to relevant policies and training alongside this policy: 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;
- never take photos of pupils on their personal devices (mobiles or cameras);
- only use smart watches (e.g. Apple watches) or Fitbits **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 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;
- maintain professional boundaries around communicating with pupils online:
    - never communicating with pupils through social media
    - only using the school email system to email pupils
    - only emailing them or responding to their emails during school hours
    - maintaining professional boundaries in emails;
- FOR OFFICE-BASED STAFF ONLY: complete a yearly Display Screen Equipment self-assessment and follow guidance about how to support good posture.

The Principal will:

- ensure that this policy is implemented consistently and effectively throughout Ivel Valley;
- make sure that the DSL accesses training to ensure that they have a good awareness of online safety.

The Designated Safeguarding Lead (DSL) will:

- support the Principal in ensuring that this policy is implemented consistently and effectively throughout Ivel Valley;
- 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);
- lead on sharing relevant online safety information with parents / carers;
- include relevant information about online safety in safeguarding reports to governors.

The Network Manager will:

- put in place an appropriate level of security protection procedures, such as filtering and monitoring systems;
- review and update these system 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 our 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;
- liaise with the DSL or Principal regarding any concerns that they identify in connection with online safety or cyberbullying.

The Understand the World area of learning lead/s 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;
- support the DSL in raising parent/carer awareness;
- support teachers to access appropriate and exciting resources.

Governors will:

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

WE NEED TO BE AWARE OF: WHAT DO WE EXPECT OUR PUPILS TO DO?

We expect our pupils to:

- 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 technology that they use;
- use technology in a safe and appropriate way.

This is our accessible online safety policy 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.

WE NEED TO BE AWARE OF: WHAT DO WE EXPECT OUR FAMILIES TO DO?

We expect our families to:

- 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 or ParentMail that are relevant to them;
- contact our Network Manager if help is needed to set filters etc.;
- take steps to ensure that their child doesn't access inappropriate content.

WE NEED TO BE AWARE OF: SPECIFIC INFORMATION

Acceptable internet use

- Staff are all expected to sign an agreement regarding appropriate use of IT and the internet, and must comply with this.
- Pupils and students from KS3 upwards will be expected to sign an accessible agreement, if appropriate.
- Visitors will be expected to read and agree to our terms on acceptable use 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 Network Manager will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

Cyberbullying or online abuse

- Children can abuse their peers online through:
    - Abusive, harassing, and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- 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.
- 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.
- The safeguarding policy contains specific guidance around youth produced sexual imagery.
- If needed, the behaviour policy will be followed to manage incidents of bullying.
- Online abuse is covered in initial safeguarding training, and is constantly reflected on through weekly safeguarding update emails.

Examining electronic devices

School 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

- Some pupils bring personal devices into school to use whilst on bus or taxi journeys. This is acceptable, but families must be aware that Ivel Valley cannot be responsible for ensuring the safety of these devices.
- Pupils are encouraged to keep personal devices in a safe place throughout the day, for example the office are able to store mobile phones.
- Pupils must not use personal devices throughout the day, unless there is a specific need for them as a learning tool, for example as a communication aid.
- 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, as explored above.

APPENDICES

ONE: Government guidance on educating pupils about online safety

TWO: Online safety risk assessment

THREE: Prevent specific risk assessment

FOUR: Links to national and school documents

APPENDIX ONE: government guidance on educating pupils about online safety

The information below comes from The Key's model online safety policy, and is taken from the National Curriculum computing programmes of study, and the guidance on relationships and sex education (RSE) and health education. This is here as a reference point – as all pupils at Ivel Valley have SEND, teachers will follow our adapted curriculum and programmes of study.

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

All schools have to teach:

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

In **Key Stage 1**, pupils 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

Pupils 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

By **the end of primary school**, pupils 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

In **Key Stage 3**, pupils 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

Pupils 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

By **the end of secondary school**, pupils 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)

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

APPENDIX TWO: 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	• Acceptable Use 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 mechanism • Appropriate monitoring • Online safety teaching & learning • DSL and Area of Learning lead 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	• Acceptable Use Agreement • Safeguarding policy • Infrastructure security • Appropriate monitoring • Online safety teaching & learning • DSL and Area of Learning lead work to identify SEND-specific resources
Cyber and Information Security	• Data Protection – data loss or compromised • Security Intrusion – information or access is compromised e.g. hack or virus/malware	Staff	• Data Protection Policy • Password policy • Data Protection Officer • Firewall security • Protective systems (anti- virus) • Software updating regime

			• Incident management
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 • UKSIC Helpline

APPENDIX THREE: 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.
Does the policy make explicit how Prevent concerns should be reported within school?			We give our staff clear information to report all concerns through CPOMS, which ensures consistency. In Central Bedfordshire, any concerns connected to radicalisation would follow the same referral process as other safeguarding concerns, i.e. through Access & Referrals.
Are Fundamental British Values (FBV) considered in curriculum planning?	Yes	SLT	Our curriculum was designed in-house, and FBV were integrated into the development process. In addition: Personal, Social & Emotional Development is one of our prime areas of learning; Understanding the World is one of our specific areas. Ongoing development of FBV-related provisions is in our School Improvement & Development Plan

			Diversity has been a significant area of focus and development
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 have accessed to. We have experience in managing SARs.
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 follow clear procedures to verify their identify. Our premises are currently only used by established local charities that provide disability support, or by groups connected to health or social care partners.
Have ALL staff received appropriated training on Prevent?	Yes	DSL	All staff – including support staff – complete Prevent training as part of their induction. Prevent is also referred to in initial safeguarding training. Relevant updates are shared throughout the year in safeguarding update emails, and Prevent is updated yearly.
Does the E-Safety Policy refer to the requirements of the Prevent guidance?	Yes	DSL	This risk assessment is appended to the online safety policy to firmly connected Prevent strategy with online safety. The policy also clearly reflects the need for appropriate filtering that blocks access to

			dangerous or extremist websites.
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.
Clear guidance on governing the display of materials internally at the school	Yes	SLT	There is display guidance for classrooms and this is monitored by the Assistant Principals. There is not a culture of staff displaying their own materials in the staffroom; this is monitored.

APPENDIX FOUR: links to local, national & school documents

Relevant school policies:

- Code of conduct
- Confidentiality policy
- Data protection and use of IT agreement
- Data protection policy
- Remote learning policy
- Safeguarding & child protection policy
- Staff handbook

National documents:

- Cyber bullying: advice for headteachers and school staff (DfE, July 2017)
- Keeping Children Safe in Education (DfE, September 2021)
- Preventing and tackling bullying (DfE, July 2017)
- Relationships Education, Relationships and Sex Education (RSE) and Health Education (DfE, September 2021)
- Searching, screening and confiscation: advice for schools (DfE, January 2018)
- Teaching online safety in school (DfE, June 2019)
- The prevent duty: for schools and childcare providers (DfE, August 2015)