Valence School
Westerham Road, Westerham, Kent. TN16 1QN
Acceptable Use of Technology Policy (AUP)

This policy has been written for…	All students, Parents/Carers, staff, visitors and Volunteers
Copies of this policy may be obtained from…	It is available as a hard copy on request from reception
Edition, Review frequency and dates	Policy reviewed: November 2022 Date agreed and ratified by Governors: 15th November 2022 Date of next review: November 2023 *This policy will be reviewed at least annually and/or following any updates to national and local guidance and procedures.*
The lead member of staff is	Lisa Kavanagh – (Vice Principal – Safeguarding & Social Care)
Key Personnel	***Roland Gooding*** (Principal) Contact details: email: rgooding@valence.kent.sch.uk tel: 01959 565627 (ext 1100) / 07896905605 ***Lisa Kavanagh*** (Vice Principal - Designated Safeguarding Lead & Head of Safeguarding & Social Care) Contact details: email: lkavanagh@valence.kent.sch.uk tel: 01959 567810 (ext 1103) / 07912 124724 ***Matt Strange*** (Vice Principal -Head of Teaching & Learning) Contact details: email: mstrange@valence.kent.sch.uk tel; 01959 562156 (ext 1102) / 07894483673 ***Jo Chivers*** (Residential Care Manager) Contact details: email: jchivers@valence.kent.sch.uk tel: 01959 567819 (ext 1104) / 07896905095 ***Zena Belton*** (Assistant Principal) Contact details: email: zbelton@valence.kent.sch.uk tel:01959 567811 (ext 1106) / 07894483666 ***Vanessa MacPherson*** (Assistant Principal) Contact details: email: vmurray@valence.kent.sch.uk Tel. 01959 562156 (ext 2270)

	Brian Davies – Chair of Governors bdavies@valence.kent.sch.uk

Ethos	Valence School community recognises that bullying, especially if left unaddressed, can have a devastating effect on individuals; it can create a barrier to learning and have serious consequences for mental wellbeing. By effectively preventing and tackling bullying, our schools can help to create safe, disciplined environment, where students are able to learn and fulfil their potential.
	
	• Our Community:
	
	    • Monitors and reviews our anti-bullying policy and practice on a regular basis.
	
	    • Supports staff to promote positive relationships, to help prevent bullying.
	
	    • Recognises that some members of our community may be more vulnerable to bullying and its impact than others; being aware of this will help us to develop effective strategies to prevent bullying from happening and provide appropriate support, if required.
	
	    • Will intervene by identifying and tackling bullying behaviour appropriately and promptly.
	
	    • Ensures our students are aware that bullying concerns will be dealt with sensitively and effectively; that everyone should feel safe to learn and abide by the anti-bullying policy.
	
	    • Requires all members of the community to work with the school to uphold the anti-bullying policy.
	
	    • Reports back to parents/carers regarding concerns on bullying, dealing promptly with complaints.
	
	    • Seeks to learn from good anti-bullying practice elsewhere.
	
	    • Utilises support from the Local Authority and other relevant organisations when appropriate.

Student Acceptable Use of Technology

Students with SEND functioning at Levels P4 –P7	• I ask a grown up if I want to use the computer • I make good choices on the computer • I use kind words on the internet • If I see anything that I don't like online, I tell a grown up • I know that if I do not follow the school rules then: My access will be reduced

Students with SEND functioning at Levels P7-L1	(Based on Childnet's SMART Rules: www.childnet.com)
	
	Safe
	• I ask a grown up if I want to use the computer
	• On the internet I don't tell strangers my name
	• I know that if I do not follow the school rules then:
	    ☐ My parents/carers will be told
	    ☐ I may not be able to use the technology
	    ☐ My access will be reduced
	Meeting
	• I tell a grown up if I want to talk on the internet

	Accepting • I do not open messages or emails from strangers. **Reliable** • I make good choices on the computer **Tell** • I use kind words on the internet • If I see anything that I don't like online, I will tell a grown up

Students with SEND functioning at Levels L2-4	(Based on Childnet's SMART Rules: www.childnet.com)
	
	Safe
	• I ask an adult if I want to use the internet
	• I keep my information private on the internet
	• I am careful if I share photos online
	• I know that if I do not follow the school rules then:
	• My parents/carers will be told
	    o I may not be able to use the technology
	    o My access will be reduced
	
	Meeting
	• I tell an adult if I want to talk to people on the internet
	• If I meet someone online, I talk to an adult
	Accepting
	• I don't open messages from strangers
	• I check web links to make sure they are safe
	Reliable
	• I make good choices on the internet
	• I check the information I see online
	Tell
	• I use kind words on the internet
	• If someone is mean online then I don't reply, I save the message and show an adult
	• If I see anything online that I don't like, I will tell a trusted adult.

Valence School – Acceptable Use of Technology
Policy (AUP)

Valence School Acceptable Use of Technology Policy – Student Agreement

I, with my parents/carers, have read and understood the Valence School Acceptable Use of Technology Policy (AUP).

I agree to follow the AUP when:

1. I use school systems and devices, both on and offsite
2. I use my own devices in school when allowed, including mobile phones, smart technology, gaming devices, and cameras.
3. I use my own equipment out of the school, including communicating with other members of the school or when accessing school systems

Name…………………………………………………

Class……………………… Date……………………

Parent/Carers Name……………………………………………......

Parent/Carers Signature…………………………

Date……………

Acceptable Use of Technology for Parents/Carers

Parent/Carer Acknowledgement Form

Student Acceptable Use of Technology Policy: Valence School Parental Acknowledgment	- I have read and discussed Valence School student acceptable use of technology policy (AUP) with my child and understand that the AUP will help keep my child safe online. - I understand that the AUP applies to my child's use of school devices and systems on site and at home and personal use where there are safeguarding and/or behaviour concerns. This may include if online behaviour poses a threat or causes harm to another student, could have repercussions for the orderly running of the school, if a student is identifiable as a member of the school, or if the behaviour could adversely affect the reputation of the school - I am aware that any use of school devices and systems are appropriately filtered and may be monitored for safety and security reasons to keep my child safe and to ensure policy compliance. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation. - I am aware that the school mobile and smart technology policy states that my child can use personal device and mobile and smart technology on site, under certain conditions and circumstances. - I understand that my child needs a safe and appropriate place to access remote/online learning, for example, if the school is closed in response to Covid-19. I will ensure my child's access to remote/online learning is appropriately supervised and any use is in accordance with the school remote learning AUP - I understand that the school will take every reasonable precaution, including implementing appropriate monitoring and filtering systems, to ensure my child is safe when they use school devices and systems. I understand that the school cannot ultimately be held responsible for the nature and content of materials accessed online or if my child is using personal mobile or smart technologies. - I and my child are aware of the importance of safe online behaviour and will not deliberately upload or share any content that could upset, threaten the safety of or offend any member of the school/setting community, or content that could adversely affect the reputation of the school/setting. - I understand that the school will contact me if they have concerns about any possible breaches of the AUP or have any concerns about my child's safety online. - I will inform the school (for example speaking to a member of staff and/or the Designated Safeguarding Lead) or other relevant organisations if I have concerns over my child's or other members of the school community's safety online. - I know that my child will receive online safety education to help them understand the importance of safe use of technology and the internet, both in and out of school - I understand my role and responsibility in supporting the school online safety approaches and safeguarding my child online. I will use parental controls, supervise access and will encourage my child to adopt safe use of the internet and other technology at home, as appropriate to their age and understanding.

Acceptable Use of Technology for Staff, Visitors and Volunteers

Staff Acceptable Use of Technology Policy

As a professional organisation with responsibility for safeguarding, all members of staff are expected to use Valence School IT systems in a professional, lawful, and ethical manner. To ensure that members of staff understand their professional responsibilities when using technology and provide appropriate curriculum opportunities for learners, they are asked to read and sign the staff Acceptable Use of Technology Policy (AUP).

Our AUP is not intended to unduly limit the ways in which members of staff teach or use technology professionally, or indeed how they use the internet personally, however the AUP will help ensure that all staff understand Valence School expectations regarding safe and responsible technology use and can manage the potential risks posed. The AUP will also help to ensure that the school systems are protected from any accidental or deliberate misuse which could put the safety and security of our systems or members of the community at risk.

Policy Scope	• I understand that this AUP applies to my use of technology systems and services provided to me or accessed as part of my role within Valence School both professionally and personally. This may include use of laptops, mobile phones, tablets, digital cameras, and email as well as IT networks, data and data storage and online and offline communication technologies. • I understand that the Valence School Acceptable Use of Technology Policy (AUP) should be read and followed in line with the school staff code of conduct, social media policy and mobile and smart technology policy, and other relevant polices. • I am aware that this AUP does not provide an exhaustive list; all staff should ensure that technology use is consistent with the school ethos, school staff behaviour and safeguarding policies, national and local education and child protection guidance, and the law.
Use of School Devices and Systems	• I will only use the equipment and internet services provided to me by the school for example school provided laptops, tablets, mobile phones and internet access, when working with students. • I understand that any equipment and internet services provided by my workplace is intended for educational use and should only be accessed by members of staff. Reasonable personal use of setting IT systems and/or devices by staff is allowed.

Data and System Security	• To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or securing/locking access.
	   o I will use a 'strong' password to access school systems.
	   o I will protect the devices in my care from unapproved access or theft by not leaving the devices visible or unsupervised in public places.
	 • I will respect school system security and will not disclose my password or security information to others.
	 • I will not open any hyperlinks or attachments in emails unless they are from a known and trusted source. If I have any concerns about email content sent to me, I will report them to the IT department
	 • I will not attempt to install any personally purchased or downloaded software, including browser toolbars, or hardware without permission from the IT department.
	
	 • I will ensure that any personal data is kept in accordance with the Data Protection legislation, including GDPR in line with the school information security policies.
	   o All personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary, and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online, or accessed remotely.
	   o Any data being removed from the school site, such as via email or on memory sticks or CDs, will be suitably protected. This may include data being encrypted by a method approved by the school.
	 •
	 • I will not keep documents which contain school related sensitive or personal information, including images, files, videos, and emails, on any personal devices, such as laptops, digital cameras, and mobile phones. Where possible, I will use the school system to upload any work documents and files in a password protected environment or school approved VPN.
	 • I will not store any personal information on the school IT system, including school laptops or similar device issued to members of staff, that is unrelated to school activities, such as personal photographs, files, or financial information.
	 • I will ensure that school owned information systems are used lawfully and appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.
	 • I will not attempt to bypass any filtering and/or security systems put in place by the school.
	 • If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the ICT Team as soon as possible.
	 • If I have lost any school related documents or files, I will report this to the ICT Team and school Data Protection Officer (Pauline Headley) as soon as possible.
	 • Any images or videos of students will only be used as stated in the school camera and image use policy.
	   o I understand images of students must always be appropriate and should only be taken with school provided equipment and taken/published where students and their parent/carer have given explicit written consent.

Classroom Practice	• I am aware of safe technology use in the classroom, safe remote learning, and other working spaces, including appropriate supervision of learners, as outlined in the school policies.

	- I have read and understood the school mobile and smart technology and social media policies. - I will promote online safety with the students in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create by: - exploring online safety principles as part of an embedded and progressive curriculum and reinforcing safe behaviour whenever technology is used on site. - creating a safe environment where students feel comfortable to say what they feel, without fear of getting into trouble and/or be judged for talking about something which happened to them online. - involving the Designated Safeguarding Lead (DSL) and deputies as part of planning online safety lessons or activities to ensure support is in place for any students who may be impacted by the content. - make informed decisions to ensure any online safety resources used with students is appropriate. - I will report any filtering breaches (such as access to illegal, inappropriate or harmful material) to the DSL in line with the school child protection/online safety policy. - I will respect copyright and intellectual property rights; I will obtain appropriate permission to use content, and if videos, images, text or music are protected, I will not copy, share or distribute or use them. .
Mobile Devices and smart technology	I will ensure that my use of mobile devices and smart technology is compatible with my professional role does not interfere with my work duties and takes place in line with the staff behaviour policy/code of conduct and the school mobile technology policy and the law.
Online communication, including use of social media	- I will ensure that my use of communication technology, including use of social media is compatible with my professional role, does not interfere with my work duties and takes place in line with the child protection/online safety policy, staff behaviour policy/code of conduct, social media policy and the law. - As outlined in the staff behaviour policy/code of conduct and school social media policy: - I will take appropriate steps to protect myself and my reputation, and the reputation of the school, online when using communication technology, including the use of social media. - I will not discuss or share data or information relating to students, staff, school business or parents/carers on social media. - My electronic communications with current and past students and parents/carers will be transparent and open to scrutiny and will only take place within clear and explicit professional boundaries. - I will ensure that all electronic communications take place in a professional manner via school approved and/or provided communication channels, such as a school email address, user account or telephone number. - I will not share any personal contact information or details with students, such as my personal email address or phone number. - I will not add or accept friend requests or communications on personal social media with current or past students and/or parents/carers. - If I am approached online by a student or parents/carer, I will not respond and will report the communication to my line manager and Designated Safeguarding Lead (DSL). - Any pre-existing relationships or situations that compromise my ability to comply with the AUP will be discussed with the DSL and/or Principal and/or Line Manager

Policy concerns	• I will not upload, download, or access any materials which are illegal, such as child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act.
	• I will not attempt to access, create, transmit, display, publish or forward any material or content online that may be harmful, is inappropriate or likely to harass, cause offence, inconvenience, or needless anxiety to any other person.
	• I will not engage in any online activities or behaviour that could compromise my professional responsibilities or bring the reputation of the school into disrepute.
	• I will report and record concerns about the welfare, safety or behaviour of students or parents/carers online to the DSL in line with the school online safety and child protection policy.
	• I will report concerns about the welfare, safety, or behaviour of staff online to the Principal/DSL, in line with school child protection policy
Policy Compliance and Breaches	• If I have any queries or questions regarding safe and professional practise online, either in school or off site, I will raise them with the DSL and/or the Principal
	• I understand that the school may exercise its right to monitor the use of its information systems, including internet access and the interception of messages/emails on our systems, to monitor policy compliance and to ensure the safety of students and staff. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.
	• I understand that if the school believe that unauthorised and/or inappropriate use of school systems or devices is taking place, the school may invoke its disciplinary procedures as outlined in the staff behaviour policy/code of conduct.
	• I understand that if the school believe that unprofessional or inappropriate online activity, including behaviour which could bring the school into disrepute, is taking place online, the school may invoke its disciplinary procedures as outlined in the staff behaviour policy/code of conduct.
	• I understand that if the school suspects criminal offences have occurred, the police will be informed.

I have read, understood and agreed to comply with the Valence School Staff Acceptable Use of Technology Policy when using the internet and other associated technologies, both on and off site.

Name of staff member: ……………………………………………………………………………

Signed: ………………………...……………………………………………………………………...

Date (DDMMYY)……………………………………………………...

Visitor and Volunteer Acceptable Use of Technology Policy

As a professional organisation with responsibility for children's safeguarding, it is important that all members of the community, including visitors and volunteers, are aware of their professional responsibilities when using technology. This AUP will help Valence School ensure that all visitors and volunteers understand the school expectations regarding safe and responsible technology use.

Policy Scope	• I understand that this Acceptable Use of Technology Policy (AUP) applies to my use of technology systems and services provided to me or accessed as part of my role within Valence School both professionally and personally. This may include use of laptops, mobile phones, tablets, digital cameras, and email as well as IT networks, data and data storage, remote learning systems and communication technologies. • I understand that the Valence School AUP should be read and followed in line with the school staff code of conduct. • I am aware that this AUP does not provide an exhaustive list; visitors and volunteers should ensure that all technology use is consistent with the school ethos, school staff behaviour and safeguarding policies, national and local education and child protection guidance, and the law.
Data and Image Use	• I will ensure that any access to personal data is kept in accordance with Data Protection legislation, including GDPR. • I understand that I am not allowed to take images or videos of students
Classroom Practice	• I am aware of the expectations regarding safe use of technology in the classroom and other working spaces, including appropriate supervision of students. • I will support staff in reinforcing safe behaviour whenever technology is used on site, and I will promote online safety with the students in my care. • I will immediately report any filtering breaches (such as access to illegal, inappropriate, or harmful material) to the Designated Safeguarding Lead (DSL) in line with the school online safety/child protection policy. • I will respect copyright and intellectual property rights; I will obtain appropriate permission to use content, and if videos, images, text, or music is protected, I will not copy, share, or distribute or use it.
Use of mobile devices and smart technology	• In line with the school mobile and smart technology policy, I understand that mobile phones and personal devices are not permitted or are only permitted within specific areas etc. I will adhere to the social media and mobile technology policy that will be available to me.

Online communication, including the use of social media	• I will ensure that my online reputation and use of technology and is compatible with my role within the school. This includes my use of email, text, social media, social networking, gaming and any other personal devices or websites.
	  o I will take appropriate steps to protect myself online as outlined in the online safety policy/child protection/social media policy.
	  o I will not discuss or share data or information relating to students, staff, school, business, or parents/carers on social media.
	  o I will ensure that my use of technology and the internet will not undermine my role, interfere with my duties and will be in accordance with the school code of conduct and the law.

	• My electronic communications with students, parents/carers and other professionals will only take place within clear and explicit professional boundaries and will be transparent and open to scrutiny.
	  ○ All communication will take place via school approved communication channels such as via a school provided email address or telephone number and not via personal devices or communication channels such as via my personal email, social networking account or mobile phone number.
	  ○ Any pre-existing relationships or situations that may compromise my ability to comply with this will be discussed with the DSL, DSL Deputies or Principal

Policy compliance, breaches, or concerns	• If I have any queries or questions regarding safe and professional practise online either in school or off site, I will raise them with the Designated Safeguarding Lead and/or the Principal • I will not upload, download, or access any materials which are illegal, such as child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act. • I will not attempt to access, create, transmit, display, publish or forward any material or content online that is inappropriate or likely to harass, cause offence, inconvenience, or needless anxiety to any other person. • I will not engage in any online activities or behaviour that could compromise my professional responsibilities or bring the reputation of the school into disrepute. • I understand that the school may exercise its right to monitor the use of school information systems, including internet access and the interception of emails/messages on school systems, to monitor policy compliance and to ensure the safety of students, staff, and visitors/volunteers. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation. • I will report and record concerns about the welfare, safety or behaviour of students or parents/carers online to the Designated Safeguarding Lead in line with the school online safety/child protection policy • I will report concerns about the welfare, safety, or behaviour of staff online to the Principal, Line Manager or DSL in line with the allegations against staff policy. • I understand that if the school believes that if unauthorised and/or inappropriate use, or unacceptable or inappropriate behaviour is taking place online, the school may invoke its disciplinary procedures. • I understand that if the school suspects criminal offences have occurred, the police will be informed.

Wi-Fi Acceptable Use Policy

As a professional organisation with responsibility for children's safeguarding it is important that all members of the school community are fully aware of the school boundaries and requirements when using the school Wi-Fi systems and take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse, and theft. This is not an exhaustive list, and all members of the school community are reminded that technology use should be consistent with our ethos, other appropriate policies, and the law.

- The school provides Wi-Fi for the school community and allows access for education and work purposes. Wi-Fi is also provided for residential boarders and is available to be used at weekends and evenings for personal use.

- I am aware that the school will not be liable for any damages or claims of any kind arising from the use of the wireless service. The school takes no responsibility for the security, safety, theft, insurance, and ownership of any device used within the school premises that is not the property of the school.

- The use of technology falls under The Valence School Acceptable Use of Technology Policy (AUP), online safety policy and child protection policy which all students/staff/visitors and volunteers must agree to and comply with.

- The school reserves the right to limit the bandwidth of the wireless service, as necessary, to ensure network reliability and fair sharing of network resources for all users.

- School owned information systems, including Wi-Fi, must be used lawfully; I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

- I will take all practical steps necessary to make sure that any equipment connected to the school service is adequately secure, such as up-to-date anti-virus software, systems updates.

- The school wireless service is not secure, and the school cannot guarantee the safety of traffic across it. Use of the school wireless service is done at my own risk. By using this service, I acknowledge that security errors and hacking are an inherent risk associated with any wireless network. I confirm that I knowingly assume such risk.

- The school accepts no responsibility for any software downloaded and/or installed, email opened, or sites accessed via the school wireless service's connection to the internet. Any damage done to equipment for any reason including, but not limited to, viruses, identity theft, spyware, plug-ins or other internet-borne programs is my sole responsibility; and I indemnify and hold harmless the school from any such damage.

- I will respect system security; I will not disclose any password or security information that is given to me. To prevent unauthorised access, I will not leave any information system unattended without first logging out or locking my login as appropriate.

- I will not attempt to bypass any of the school security and filtering systems or download any unauthorised software or applications.

- My use of school Wi-Fi will be safe and responsible and will always be in accordance with the school AUP and the law including copyright and intellectual property rights. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites.

- I will not upload, download, access or forward any material which is illegal or inappropriate or may cause harm, distress or offence to any other person, or anything which could bring the school into disrepute.

- I will report any online safety concerns, filtering breaches or receipt of inappropriate materials to the Designated Safeguarding Lead as soon as possible.

- If I have any queries or questions regarding safe behaviour online, I will discuss them with Designated Safeguarding Lead or the Principal.

- I understand that my use of the school Wi-Fi may be monitored and recorded to ensure policy compliance in accordance with privacy and data protection legislation. If the school suspects that unauthorised and/or inappropriate use or unacceptable or inappropriate behaviour may be taking place, then the school may terminate or restrict usage. If the school suspects that the system may be being used for criminal purposes, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read, understood and agreed to comply with the Valence School Wi-Fi acceptable Use Policy.

Name …………………………………………………………………………..