Policy No: 1.(c).1

The Cornwall Independent School

ONLINE SAFETY POLICY INCLUSIVE OF CYBER BULLYING, ACCEPTABLE USE AND SOCIAL MEDIA

This policy, which applies to the whole school, including the Early Years Foundation Stage (EYFS), is publicly available on the school website and upon request a copy (which can be made available in large print or other accessible format if required) may be obtained from the School Office.

Scope: All who work, volunteer or supply services to our school have an equal responsibility to understand and implement this policy and its procedures both within and outside of normal school hours, including activities away from school. All new employees and volunteers are required to state that they have read, understood and will abide by this policy and its procedural documents and confirm this by signing the *Policies Register*.

Legal Status: Complies with The Education (Independent School Standards) (England) Regulations currently in force.

Monitoring and Review: These arrangements are subject to continuous monitoring, refinement, and audit by the Headteacher. The Advisory Board will undertake a full annual review of this document, inclusive of its implementation and the efficiency with which the related duties have been implemented. This review will be formally documented in writing. Any deficiencies or weaknesses recognised in arrangements or procedures will be remedied immediately and without delay. All staff will be informed of the updated/reviewed arrangements and it will be made available to them in writing or electronically.

Signed:

Date reviewed:	November 2024
Date of next review:	September 2025

Miss L. Adams	Mr Stephen Beck	Mrs Carol de Labat
Headteacher	Chair of the Advisory Board	Advisory Board Member for Safeguarding

Introduction: The purpose of this Policy is to safeguard pupils and staff at The Cornwall Independent School. It details the actions and behaviour required from pupils and members of staff in order to maintain a safe electronic environment and is based on current best practice drawn from a wide range of sources. In accordance with legislative requirements, we have a whole school approach to Online Safety. Our key message to keep pupils and young people safe is to be promoted and should be applied to both online and offline behaviours. Within our Online Safety policy, we have clearly defined roles and responsibilities for online safety as part of the school's wider safeguarding strategy and how this links with our main Safeguarding & Child Protection Policy and other related documents. There are implications with reference to technology and Prevent Duty cited in this policy, as part of an online safety integrated policy linked to the Prevent strategy. However, it is incumbent on The Cornwall Independent School to also have a free-standing policy regarding the Preventing of Extremism and Radicalisation, that is an essential adjunct to the Online Safety Policy.

Online safety is a running and interrelated theme when devising and implementing our wider school policies and procedures, including our Safeguarding & Child Protection Policy and our Preventing Extremism and Tackling Radicalisation Policy. The staff and pupil Acceptable Use Policies (AUPs) are central to the Online Safety policy and should be consulted alongside this policy.

We consider how we can promote online safety whilst developing our curriculum, through our staff training, and also through parental engagement. The Online Safety policy will be reviewed annually by the safeguarding team who will provide recommendations for updating the policy in the light of experience and changes in legislation or technologies. The Pupil Council will be consulted regarding any changes to the Pupil AUP. All staff should read these policies in conjunction with the Online Safety policy. This is particularly important with regard to the Prevent Strategy, as a large portion of cases of radicalisation happen through the online medium. Staff must be vigilant when dealing with such matters and ensure that they observe the procedure for reporting such concerns in line with that laid out in the Safeguarding (Child Protection) Policy, Preventing Extremism and Tackling Radicalisation Policy.

Roles and Responsibilities: The Designated Safeguarding Lead (DSL)is responsible for ensuring the online safety of the school community. Our information technology coordinator (ICT) will take operational responsibility for online safety in the School, but the overall responsibility will fall on the DSL for making sure that policy is enforced and that the necessary checks, filters and monitoring are in place. The Headteacher working with the DSL, the senior leadership team and with advice from the IT coordinator have responsibility to ensure that pupils are safe from cyber bullying both within and outside the school community. Appropriate steps are taken if an incident occurs. The Leadership Team will also review online safety and the acceptable use of technology in the school during their regular meetings. The (DSL) has responsibility for ensuring that online safety is considered an integral part of everyday safeguarding practice in compliance with Keeping Children Safe in Education (KCSIE), DfE September 2023 the IT Coordinator role overlaps with that of the Online Safety Officer – the DSL, which includes ensuring that:

- Pupils know how to use the Internet responsibly and that parents and teachers have the right measures in place to keep pupils safe from exploitation or radicalisation.
- pupils are safe from terrorist and extremist material when accessing the Internet in school, including by establishing appropriate levels of filtering.
- pupils use Information and Communications Technology (ICT) safely and securely and are aware of both external and peer to peer risks when using ICT, including cyberbullying and other forms of abuse.
- children, staff, the Advisory Board and volunteers will receive the appropriate Online Safety training, guidance, time and resources to effectively implement online safety policies and procedures;
- clear and rigorous policies and procedures are to be applied to the use/non-use of personal ICT equipment by all individuals who affect or come into contact with the early years setting. Such policies and procedures are to include the personal use of work-related resources.
- the Acceptable Use Policies (AUPs) are to be implemented, monitored and reviewed regularly, and for ensuring all updates are to be shared with relevant individuals at the earliest opportunity.
- monitoring procedures are to be transparent and updated as agreed in school policies.
- allegations of misuse or known incidents are to be dealt with appropriately and promptly, in line with agreed procedures, and in liaison with other agencies, where applicable.

- effective online safeguarding support systems are to be put in place, for example, filtering controls, secure networks and virus protection to ensure that the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- an appropriate level of authorisation is to be given to ICT users. Not all levels of authorisation will be the same - this will depend on, for example, the position, work role and experience of the individual concerned.
- users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- a current record of all staff and pupils who are granted access to school ICT system is maintained.

Designated Safeguarding Lead (DSL): The Designated Safeguarding Lead (DSL) is a senior member of the management team who takes lead responsibility for online safety at The Cornwall Independent School, has relevant, current and practical knowledge and understanding of safeguarding, child protection and online safety. Access to an individual holding this role is available at all times, for example, a Deputy Designated Safeguarding Lead is also in place should the DSL be absent. At The Cornwall Independent, the DSL is the Pastoral Lead and a member of the SLT. The designated persons for safeguarding will be responsible for ensuring that:

- supporting the Headteacher and Advisory Board in ensuring that staff understand this policy and that it is being implemented consistently throughout the school;
- working with the Headteacher and Advisory Board, IT manager and other staff, as necessary, to address any online safety issues or incidents;
- ensuring that any online safety incidents are logged (see appendix 1) and dealt with appropriately in line with this policy;
- ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the School's **behaviour policy;**
- communicating any updates regarding online safety to all members of staff;
- liaising with other agencies and/or external services if necessary;
- ensuring all new staff are aware of The Cornwall Independent online safety policy during their introduction;
- providing regular reports on online safety in the School to the Headteacher and Advisory Board;
- agreed policies and procedures are to be implemented in practice.
- all updates, issues and concerns are to be communicated to all ICT users.
- the importance of online safety in relation to safeguarding is to be understood by all ICT users.
- the training, learning and development requirements of staff are to be monitored and additional training needs identified and provided for.
- the learning and development plans of pupils and young people will address online safety.
- a safe ICT learning environment is to be promoted and maintained.

The above list is not intended to be exhaustive and will be amended as is appropriate

Not all levels of authorisation will be the same - this will depend on, for example, the position, work role and experience of the individual concerned. In some instances, explicit individual authorisation must be obtained for specific activities when deemed appropriate, and any concerns and incidents are to be reported in a timely manner in line with agreed procedures. The learning and development plans of students and young people will address online safety. A safe ICT learning environment is to be promoted and maintained.

The Proprietor's responsibilities: Whilst considering their responsibility to safeguard and promote the welfare of children and provide them with a safe environment in which to learn, the proprietor will do all that they reasonably can to limit children's exposure to risks when using the school's IT system. As part of this process, the proprietor has ensured the school has appropriate filters and monitoring systems in place which are reviewed regularly to monitor their effectiveness. They ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place, how to manage them effectively and know how to escalate concerns when identified.

All Staff: It is the responsibility of all staff to be alert to possible harm to pupils or staff due to inappropriate Internet access or use, both inside and outside of The Cornwall Independent School, and to deal with incidents of such as a priority. All staff are responsible for ensuring they are up to date with current online safety issues, and this online Safety Policy. Cyber-bullying incidents will be reported in accordance with The Cornwall Independent School's Anti-Bullying Policy. All staff will ensure they understand and adhere to our staff Acceptable Use Policy, which they must sign and return to the Online Safety Officer which will be placed on staff files. Teachers will ensure they are confident in promoting and delivering online safety as required, identifying risks and reporting concerns as they arise.
Additionally the following is incumbent on all staff:

- working with the DSL and/or **prevent lead** to ensure that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy;
- ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the School's **behaviour policy;**
- engage with new safety information and updates, for example at staff meetings or those received via email;

The above list is not intended to be exhaustive and will be amended as is appropriate

Parents/Carers: Parents/carers are responsible for ensuring their child understands how to use computer technology and other digital devices appropriately. The Cornwall Independent School will support parents/carers by sharing information and links through newsletters, the school's website, Microsoft Teams and through formal/informal training.
Additionally, the following is incumbent on all parents:

- notify a member of staff or the Headteacher of any concerns or queries regarding this policy;
- ensure their child has read, and understood and agreed to the terms on **acceptable use agreement** of the School's IT systems and internet (appendix 1);
- engage with our online safety guidance which is regularly shared with parents through our website, newsletters, social media platforms and regular safety briefings via email, raising any concerns that they have.

Parents can seek further guidance on keeping children safe online from the following organisations and websites:
what are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues

- hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- parent factsheet, Childnet international: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

visitors and members of the community: visitors and members of the community who use the School's IT systems or internet will be made aware of this policy, when relevant, and are expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use agreement (appendix 2).

All Pupils: All pupils will ensure they understand and adhere to our pupil Acceptable Use Policy, which they must sign and return to the DSL. Pupils are reminded of their responsibilities regarding the use of the school's ICT systems and equipment, including their expected behaviour.

Breadth of Online Safety Issues: We classify the issues within online safety into **four** areas of risk:

- **Content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- **Contact:** being subjected to harmful online interaction with other users; for example: peer to peer 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; for example, 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; and
- **Commerce** - risks such as online gambling, inappropriate advertising, phishing and or financial scams.

These issues are to be managed through the school's filtered Internet, by promoting safe and responsible use, and ensuring both staff and pupils are able to report any concerns to the appropriate people.

Staff/Volunteers Use of IT Systems: Access to the Internet and e-mail is provided to support the curriculum, support school administration and for staff professional development only. All staff must read and confirm by signature that they have read the 'Staff Code of Conduct for ICT) (please see appendices) before using any school ICT resource. In addition:

- All staff including the Proprietor and Advisory Board will receive appropriate Online Safety training, which is updated regularly;
- Online Safety issues are embedded in all aspects of the curriculum and other activities.
- Access to systems should be made by authorised passwords, which must not be made available to any other person.
- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse, using personal data only on secure password-protected computers and other devices.
- In lessons where Internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches.
- Where pupils are allowed to freely search the Internet, staff should be vigilant in monitoring the content of the websites the pupils visit.
- Occasionally pupils may need to research educational material that may normally result in websites being blocked (e.g. racism). In this situation, staff may request to remove these sites form the filtered list for the period of study. Any request to do so should be made to the IT Coordinator.
- The Internet can be used to actively gather personal information about individuals which may lead to undesirable consequences (e.g. SPAM, fraud, harassment or identity theft). Because of this, staff are advised to only use the school approved software and email systems which have appropriate security in place.
- Files should not be saved directly from the Internet unless they can first be scanned for computer viruses, malware, spyware and other malicious programmes;
- Staff should only communicate electronically with pupils through the school approved platforms. This includes the school VLE (FROG), and additionally in KS3 & 4 via the school's Google Workspace for Education platform.
- Educational materials made by and for classes and uploaded to password-protected YouTube channels, i.e. videos of lessons, activities, or fieldtrips, should be logged for record-keeping purposes. This provides an opportunity to share best practices and resources and enable better teaching and learning outcomes.

Any person suspecting another of deliberate misuse or abuse of technology should take the following action:

1. Report in confidence to the school's member of staff who is responsible for online safety, who is the DSL
2. The Online Safety Officer should investigate the incident.
3. If this investigation results in confirmation of access to illegal material, the committing of illegal acts, or transgression of school rules, appropriate sanctions will be enforced.
4. In exceptional circumstances, where there are reasonable grounds to suspect that a user has committed a serious criminal offence, the Child Exploitation and Online Protection Command (CEOP) and the police will be informed.
5. No pupil or member of staff should attempt to access or view the material, whether online or stored on internal or external storage devices. If this step is necessary, CEOP and the police will be contacted.

Teaching about Online Safety: Our Online Safety Curriculum is closely linked with our Relationships and Sex Education Programme and discusses the links associated with Online abuse and other associated risks. Because new opportunities and challenges appear all the time, it is important that we focus our teaching on the underpinning knowledge and behaviours that can help pupils to navigate the online world safely and confidently regardless of the device, platform or app. Online Safety is a focus in all areas of the curriculum and key Online Safety messages are reinforced regularly, teaching pupils about the risks of Internet use, how to protect themselves and their peers from potential risks, how to recognise suspicious, bullying or extremist behaviour and the consequences of negative online behaviour. Access levels to ICT reflect the curriculum requirements and age of pupils. Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and maturity. This teaching is built into existing lessons alongside our wider whole-school approach. Pupils will explicitly be taught the following topics through their lessons:

- What Internet use is acceptable and what is not and given clear guidelines for Internet use including protecting their online identity and privacy;
- How to use a wide range of devices and learn about their advantages and disadvantages, in different applications;
- How to evaluate what they see online;
- How to recognise techniques used for persuasion;
- Online behaviour;
- How to identify online risks and

- How and when to seek support.
- How to recognise and respond to harmful online challenges and online hoaxes.

We recognise that Peer-on-Peer abuse can occur online and to this end we teach pupils how to spot early warning signs of potential abuse, and what to do if pupils are subject to sexual harassment online. When accessing the Internet individuals are especially vulnerable to a number of risks which may be physically and emotionally harmful, including:

- Access to illegal, harmful or inappropriate images
- Cyber bullying
- Access to, or loss of, personal information
- Access to unsuitable online videos or games
- Loss of personal images
- Inappropriate communication with others
- Illegal downloading of files
- Exposure to explicit or harmful content, e.g. involving radicalisation
- Plagiarism and copyright infringement
- Sharing the personal information of others without the individual's consent or knowledge

Staff should be vigilant in lessons where pupils use the Internet. If staff allow the use of mobile devices in their lessons, they must ensure that they are used in line with school policy.

Harmful online challenges and online hoaxes: (Please refer to the latest DfE Guidance) There has been a growing trend in the number of both challenges and hoaxes online as well as their popularity. As such, the school has put in a number of measures to safeguard our children. A hoax is a deliberate lie designed to seem truthful, and online challenges generally involve users recording themselves taking a challenge, and then distributing the video through social media channels, inspiring or daring others to repeat the challenge. We teach pupils to recognise the signs that something may be untruthful online or that risks associated with any online challenges as well as who they can speak to if they have a concern. Where a child or member of staff reports an online hoax or challenge, we ensure that they are taken seriously, and acted upon appropriately, with the best interests of the child coming first. We ensure we provide opportunities to discuss this topic within Online Safety lessons, ensuring children and young people can ask questions and share concerns about what they experience online without being made to feel foolish or blamed.

A case-by-case assessment, establishing the scale and nature of the possible risk to our students will be carried out, and appropriate actions taken, which may include sharing information with parents and carers, our own young people as well as other local schools. Forward planning, together with case-by-case research, will allow for a calm and measured response and avoid creating panic or confusion by spreading information which itself is untrue or would only draw students' attention to a potential risk.

Our DSL will check the factual basis of any harmful online challenge or online hoax with a known, reliable and trustworthy source, such as the Professional Online Safety Helpline from the UK Safer Internet Centre. Where harmful online challenges or online hoaxes appear to be local (rather than large scale national ones) local safeguarding advice, such as from the local authority or local police force, may also be appropriate and helpful. Information that is shared with parents and carers will include encouraging them to focus on positive and empowering online behaviours with their children, such as critical thinking, how and where to report concerns about harmful content and how to block content and users.

Pupils Use of IT Systems: All pupils must agree to the IT Acceptable Use Policy before accessing the school systems. Pupils at The Cornwall Independent School will be given supervised access to our computing resources and will be provided with access to filtered Internet and other services operating at the school. Problems with ICT equipment should be reported either to the class teacher or the IT Coordinator. The promotion of online safety within ICT activities is to be considered essential for meeting the learning and development needs of pupils and young people. The school will ensure that the use of Internet-derived materials by staff and pupils complies with copyright law. The Cornwall Independent School will help pupils to understand the risks posed by adults or young people, who use the Internet and social media to bully, groom, abuse or radicalise other people, especially pupils, young people and vulnerable adults. Internet safety is integral to the school's ICT curriculum and is also be embedded in our Personal, Social, Health and Economic

Education (PSHEE) and Spiritual, Moral, Social and Cultural (SMSC) Development. The latest resources promoted by the DfE can be found at:

- Education for a connected world
- The UK Safer Internet Centre (www.saferinternet.org.uk)
- CEOP's Thinkuknow website (www.thinkuknow.co.uk)
- Teaching Online Safety in School https://www.gov.uk/government/publications/teaching-online-safety-in-schools
- Google Legends (KS2) (https://beinternetlegends.withgoogle.com/en_uk)

Educating Staff: Staff and the Advisory Board will be provided with sufficient online safety training to protect pupils and themselves from online risks and to deal appropriately with Online Safety incidents when they occur. Ongoing staff development training includes training in online safety, together with specific safeguarding issues including cyberbullying and radicalisation. The frequency, level and focus of such training will depend on individual roles and requirements. Staff will undergo online safety training annually/when changes occur basis to ensure they are aware of current online safety issues and any changes to the provision of online safety, as well as current developments in social media and the Internet as a whole. All staff will employ methods of good practice and act as role models for young people when using the Internet and other digital devices. All staff will be educated on which sites are deemed appropriate and inappropriate. All staff are reminded of the importance of acknowledging information they access online, in order to avoid copyright infringement and/or plagiarism. Any new staff are required to undergo online safety training as part of their induction program, ensuring they fully understand this online safety policy/social media policy/user agreement. The Online Safety Officer will act as the first point of contact for staff requiring online safety advice.

Communicating and Educating parents/carers in online safety: We believe that it is essential for parents/carers to be fully involved with promoting online safety both in and outside of school and to be aware of their responsibilities. We regularly consult and discuss online safety with parents/carers and seek to promote a wide understanding of the benefits of new technologies, together with the associated risks. For example, parents/carers are required to make a decision as to whether they consent to images of their child being taken and used in the public domain (e.g., on School website). Parents/carers will also be provided with a copy of the age-relevant Pupil IT Acceptable Use Policy, and parents/carers will be asked to sign it, as well as the pupils. The Cornwall Independent School recognises the crucial role that parents/carers play in the protection of their children with regards to online safety. The school organises an annual awareness session for parents/carers with regards to online safety which looks at emerging technologies and the latest ways to safeguard pupils from inappropriate content. The school will also provide parents/carers with information through newsletters, and the school VLE, which is FROG. Parents/carers are always welcome to discuss their concerns on online safety with the school, who can direct them to the support of our Online Safety Officer if required. Parents/carers will be encouraged to support the school in promoting good online safety practice.

Cyber Security: The School recognises its responsibility to ensure that appropriate security protection procedures are in place to safeguard are systems. As part of our whole-school Online Safety Training, we ensure staff, governance advisory committee and proprietor are updated with the evolving cyber-crime technologies. In addition, the school activity considers the Cyber security standards (DfE: 2023) and uses these as a base for keeping the school and its community safe from cyber-crime**.**

Characteristics of a strong password

- at least 8 characters – the more characters the better;
- a mixture of both uppercase and lowercase letters;
- a mixture of letters and numbers;
- inclusion of at least one special character e.g. !@#?]

note: do not use < or > in your password, as both can cause problems in web browsers.
A strong password is hard to guess, but it should be easy for you to remember – a password that has to be written down is not strong, no matter how many of the above characteristics are employed

Protecting Personal Data: Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 and the UK General Data Protection Regulations (GDPR) 2020. The school recognises that if required, data may need to be obtained by relevant parties such as the Police. Pupils are encouraged to keep their personal data private as part of our online safety lessons and IT curriculum, including areas such as password protection and knowledge about apps and unsecured networks/apps etc. The school will be responsible for ensuring there is an appropriate level of security procedures in place, in order to safeguard systems, staff and learners and will review the effectiveness of these procedures periodically to keep up with evolving cyber-crime technologies.

Technology and Prevent Duty: As part of an integrated policy linked to the Prevent strategy, the School also has a duty to ensure that pupils are prevented and protected from the risk of being radicalised through the access to extremist propaganda, e.g. from ISIL. The School must promote British values through the curriculum and SMSC and SRE. Teachers must also be aware of their responsibility to monitor and report any serious concerns they have about a pupil's use or access to inappropriate material, especially that which undermines British values and tolerance of others. The School's network and facilities must NOT be used for the following activities:

- Accessing or downloading pornographic material
- Gambling
- Accessing sites or social media channels that promote extreme viewpoints and radical propaganda
- Gambling
- Soliciting for personal gain/profit
- Revealing or sharing proprietary or confidential material
- Representing personal opinions about the School
- Positing indecent or humiliating images or remarks/proposals

We ensure pupils are safe from terrorist and extremist material when accessing the Internet in school, including by ensuring suitable filtering is in place. The DfE advises that Internet safety will usually be integral to the ICT curriculum and can also be embedded in PSHEE, for example. Every teacher needs to be aware of the risks posed by online activity of extremist and terrorist groups. For further information, please refer to our *'Preventing Extremism and Radicalisation'* Policy.

Radicalisation and the Use of Social Media to Encourage Extremism: The Internet and the use of social media in particular has become a major way to communicate with others, especially young people, which has provided access for like-minded people to create an online community and promote extreme beliefs, sharing extreme ideological views or advocating the use of violence to solve problems. This has led to social media becoming a platform for:

- intensifying and accelerating the radicalisation of young people;
- promoting extreme beliefs;
- accessing likeminded people where they are not able to do this off-line, creating an online community;
- normalising abnormal views and behaviours, such as extreme ideological views or the use of violence to solve problems and address grievances.

The Cornwall Independent School has a number of measures in place to help prevent the use of social media for this purpose:

- Website filtering is in place to help prevent access to terrorist and extremist material and social networking sites such as Facebook, Instagram or Twitter by pupils.
- Pupils, parents/carers and staff are educated in safe use of social media and the risks posed by online activity, including from extremist and terrorist groups.

Further details on how social media is used to promote extremism and radicalisation can be found in guidance from the Department for Education '*How Social Media Is Used to Encourage Travel to Syria and Iraq: Briefing Note for Schools.'*

Reporting of Online Safety Issues and Concerns Including Concerns Regarding Radicalisation: The Cornwall Independent School has clear reporting mechanisms in place, available for all users to report issues and concerns. For staff, any concerns regarding online safety should be made to the Online Safety Officer, who will review the issue and take the appropriate action. For pupils, they are taught to raise any concerns to their class teacher who will then pass this on to the Online Safety Officer. Complaints of a child protection nature must be dealt with in accordance with our Safeguarding & Child Protection Policy.

Our Designated Safeguarding Lead (DSL) provides advice and support to other members of staff on protecting pupils from the risk of online radicalisation. The Cornwall Independent School ensures staff understand what radicalisation and extremism mean and why people may be vulnerable to being drawn into terrorism. We ensure staff have the knowledge and confidence to identify pupils at risk of being drawn into terrorism, and to challenge extremist ideas, which can be used to legitimise terrorism. Staff safeguard and promote the welfare of pupils and know to report any concerns to the DSL.

Assessing Risks:

- We will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. The school cannot accept liability for any material accessed, or any consequences of Internet access.
- Developing technologies, such as mobile phones with Internet access are not governed by the school's infrastructure and can bypass any and all security and filtering measures that are or could be deployed. We recognise the additional risks this has for our pupils, who could have unsupervised access to the Internet when using their own devices. To address this, the school works with pupils across our age range to ensure that pupils are educated clearly about the risks of both social media and Internet use, alongside regularly monitoring of device usage as appropriate.
- We will audit ICT use to establish if the Online Safety policy is sufficiently robust and that the implementation of the Online Safety policy is appropriate and effective.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The Advisory Board will review and examine emerging technologies for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Any person not directly employed by the school will not be provided with access to any of the school systems with the exception of filtered *Wi-Fi* access, if necessary.
- The Cornwall Independent School takes measures to ensure appropriate IT filters monitoring systems are in place to safeguard pupils from potentially harmful and inappropriate material on-line without unreasonable "over-blocking"
- The school recognises that students may choose to circumvent certain safety precautions by using mobile data on their devices over 3G, 4G and 5G. To help provide a safe environment for all students, we will supplement the systems filtering with behaviour management and additional staff/student training. Pupils must place any personal mobile devices in the school office when arriving at school and may collect them on their way out at the end of the day.

Emerging technologies, such as mobile phones with internet access (smartphones) are not governed by the school's infrastructure and bypass any and all security and filtering measures that are or could be deployed. We recognise the additional risks this has for our pupils in Boarding, who could have unsupervised access to the internet when using their own devices in their free time. To address this, the School works with pupils across our age range to ensure that pupils are educated clearly about the risks of both social media and internet use, alongside regularly monitoring of device usage as appropriate.

Filtering and Monitoring: The School provides a safe environment for pupils to learn and work in, especially when online. Filtering and monitoring are both important parts of safeguarding pupils from potentially harmful and inappropriate online material. The proprietor has overall strategic responsibility for filtering and monitoring. For this to occur, they have assigned a member of the senior leadership team (the DSL) and the Advisory Board to be responsible for ensuring the se standards are met. The DSL works closely with IT lead and other member of SLT to ensure that filtering and monitoring is adequate and robust in the School and boarding facility. The School considers those who are potentially at greater risk of harm and how often they access the School's IT systems. The School follows the Filtering and Monitoring Standards (DFE 2023) which ensures that the School:

- identifies and assigns roles and responsibilities to manage filtering and monitoring systems;
- reviews filtering and monitoring provision at least annually;
- blocks harmful and inappropriate content without unreasonably impacting teaching and learning;
- has effective monitoring strategies in place that meet the school's safeguarding needs.

Phishing and Pharming Definition: A phishing email usually contains a link with directions asking the recipient to click on it. Clicking the link transports the email recipient to an authentic looking, albeit fake, web page. The target is asked to input information like a username and password, or even additional financial or personal data. The miscreant that orchestrates the phishing scheme is able to capture this information and use it to further criminal activity, like theft from a financial account and similar types of criminal activity.

Pharming is the term used to describe a cyber scam where malicious code redirects a user to a fake website without their knowledge, with the intention of stealing confidential information. As opposed to phishing, pharming requires an attacker to gain unauthorised access to a system. **The School has no intention of changing its financial information, therefore never accept an email with a link pretending to be the School's accounts department.**

Top tips:

- Never click on hyperlinks in email from an unknown sender, rather manually type the URL into the web browser itself
- Never enter sensitive information in a pop-up window except at those sites that an individual knows to be trustworthy
- Verify HTTPS on the address bar - whenever a person is conveying confidential information online, you must confirm that the address bar reads "HTTPS" and not the standard "HTTP." The "S"confirms that the date is being conveyed through a legitimate, secured channel
- Access personal and financial information only from a computer or device you trust to be free from trojans and keyloggers
- Education on phishing and pharming attacks - staying abreast of phishing scams and the technologyand techniques designed to prevent them is crucial. A plethora of reliable educational resourcesexist on the Internet that are designed to assist a person in preventing phishing attacks
- Report phishing and pharming to the financial institution, the FTC, and the Internet Crime Complaint Centre

Mobile Electronic Devices (Phones, Laptops, iPads and Tablets; please see appendix 3 for more details): Mobile telephones are not permitted to be used by pupils during the school day. Pupils must leave their mobile devices in the school office upon arrival and collect them at the end of the school day. Pupils may go to the school office during break times to check their devices. Mobile phones are kept on site at the risk of the individual pupil. The Cornwall Independent School is not responsible for any devices lost or damaged whilst on school grounds.

Recordings made using mobile electronic devices: Using the camera on a phone or similar device, either to photograph/film/record any member of the school community, do any form of live streaming or to show to others the photos/videos/audio recordings already on the phone or similar device is prohibited. The discovery of any uploads to social media platforms will result in serious sanctions being applied.

Cyber-Bullying: like other forms of bullying, cyber-bullying is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (please see also the School's behaviour policy.) Cyber-bullying (along with all forms of bullying) will not be tolerated and incidents of cyberbullying should be reported and will be dealt with in accordance with the School's Anti-Bullying Policy. Cyberbullying (along with all forms of bullying) will not be tolerated and incidents of cyberbullying should be reported and will be dealt with in accordance with the School's Anti-Bullying Policy. Use of electronic devices of any kind to bully, harass or intimidate others will not be tolerated and will constitute a serious breach of discipline. If there is a suggestion that a child is at risk of abuse or significant harm, the matter will be dealt with under the school's child protection procedures (see our Safeguarding & Child Protection Policy). Seven categories of cyber-bullying have been identified:

- **Text message bullying** involves sending unwelcome texts that are threatening or cause discomfort;
- **Picture/video-clip bullying via mobile phone cameras** is used to make the person being bullied feel threatened or embarrassed, with images usually sent to other people. 'Happy slapping' involves filming and sharing physical attacks;
- **Phone call bullying via mobile phone** uses silent calls or abusive messages. Sometimes the bullied person's phone is stolen and used to harass others, who then think the phone owner is responsible. As with all mobile phone bullying, the perpetrators often disguise their numbers, sometimes using someone else's phone to avoid being identified;
- **Email bullying** uses email to send bullying or threatening messages, often using a pseudonym for anonymity or using someone else's name to pin the blame on them;
- **Chat room bullying and online grooming** involve sending menacing or upsetting responses to pupils or young people when they are in a web-based chat room;
- **Bullying through instant messaging (IM)** is an Internet-based form of bullying where pupils and young people are sent unpleasant messages through various messaging applications (for example, WhatsApp, Group Me, Skype, Facebook Messenger, Snapchat, text messaging etc.) as they conduct real-time conversations online;
- **Bullying via websites and social networks (an example of this would be Facebook, Twitter, Instagram, etc.)** includes the use of defamatory blogs, personal websites and online personal polling sites. There has also been a significant increase in social networking

sites for young people, which can provide new opportunities for cyber-bullying.

Pupils should remember the following:

- Always respect others - be careful what you say online and what images you send.
- Think before you send - whatever you send can be made public very quickly and could stay online forever.
- Don't retaliate or reply online.
- Save the evidence - learn how to keep records of offending messages, pictures or online conversations. Ask someone if you are unsure how to do this. This will help to show what is happening and can be used by the school to investigate the matter.
- Block the bully. Most social media websites and online or mobile services allow you block someone who is behaving badly.
- Do something - if you see cyberbullying going on, support the victim and report the bullying.

Online Sexual Harassment: Sexual harassment creates an atmosphere that, if not challenged, can normalise inappropriate behaviours and provide an environment that may lead to sexual violence. online sexual harassment include: non-consensual sharing of sexual images and videos and sharing sexual images and videos (both often referred to as sexting); inappropriate sexual comments on social media; exploitation; coercion and threats. Online sexual harassment may be standalone, or part of a wider pattern of sexual harassment and/or sexual violence. All cases or allegations of sexual harassment, online or offline, is unacceptable and will dealt with under our Child Protection Procedures.

Additionally, we recognise that incidents of sexual violence and sexual harassment that occur online (either in isolation or in connection to offline incidents) can introduce a number of complex factors. These include the potential for the incident to take place across a number of social media platforms and services and for things to move from platform to platform online. It also includes the potential for the impact of the incident to extend further than the school's local community (e.g. for images or content to be shared around neighbouring schools/colleges) and for a victim (or alleged perpetrator) to become marginalised and excluded by both online and offline communities. There is also the strong potential for repeat victimisation in the future if abusive content continues to exist somewhere online. Online concerns can be especially complicated. Support is available at:

- The UK Safer Internet Centre provides an online safety helpline for professionals at 0344 381 4772 and helpline@saferInternet.org.uk. Providing expert advice and support for school staff with regard to online safety issues and when an allegation is received.
- If the incident involves sexual images or videos that have been made and circulated online, we will support the victim to get the images removed through the Internet Watch Foundation (IWF). The IWF will make an assessment of whether the image is illegal in line with UK Law. If the image is assessed to be illegal, it will be removed and added to the IWF's Image Hash list.

ICT-Based Sexual Abuse (Including Sexting): The impact on a child of ICT-based sexual abuse is similar to that for all sexually abused pupils. However, it has an additional dimension in that there is a visual record of the abuse. ICT-based sexual abuse of a child constitutes significant harm through sexual and emotional abuse. Recognition and response is recognising a situation where a child is suffering, or is likely to suffer a degree of physical, sexual and/or emotional harm (through abuse or neglect) which is so harmful that there needs to be compulsory intervention by child protection agencies into the life of the child and their family. All adults (volunteers, staff) working with pupils, adults and families will be alerted to the possibility that:

- A child may already have been/is being abused and the images distributed on the Internet or by mobile telephone;
- An adult or older child may be grooming a child for sexual abuse, including involvement in making abusive images. This process can involve the child being shown abusive images;
- An adult or older child may be viewing and downloading child sexual abuse images.

Pupils are reminded that 'sexting' (sending or posting images or videos of a sexual or indecent nature) is strictly prohibited by the school and may constitute a criminal offence. The school will treat incidences of sexting (both sending and receiving) as a safeguarding issue and pupils concerned about images that they have received, sent or forwarded should speak to any member of staff for advice.

There are no circumstances that will justify adults possessing indecent images of pupils. Adults who access and possess links to such websites will be viewed as a significant and potential threat to pupils. Accessing, making and storing indecent images of pupils is illegal.

This will lead to criminal investigation and the individual being barred from working with pupils, if proven. Adults should not use equipment belonging to the school to access adult pornography; neither should personal equipment containing these images or links to them be brought into the workplace. This will raise serious concerns about the suitability of the adult to continue to work with pupils. Adults should ensure that pupils are not exposed to any inappropriate images or web links. Where indecent images of pupils or other unsuitable material are found, the police and Local Authority Designated Officer (LADO) should be immediately informed. Adults should not attempt to investigate the matter or evaluate the material themselves, as this may lead to evidence being contaminated, which in itself can lead to a criminal prosecution.

Sanctions: Sanctions will depend on the severity of the offence as assessed by the Senior Leadership Team. They may include one or more of the following:

- Temporary or permanent ban on the use of ICT resources in the School.
- Temporary or permanent ban on the use of the Internet in the School.
- Additional disciplinary action may be added in line with existing practice on inappropriate language or behaviour.
- Temporary or permanent exclusion from school may be imposed.
- If appropriate, police or local authorities may be involved.

Chat Room Grooming and Offline Abuse: Our staff need to be continually alert to any suspicious activity involving computers and the Internet. Grooming of pupils online is a faster process than usual grooming, and totally anonymous. The abuser develops a 'special' relationship with the child online (often adopting a false identity), which remains a secret to enable an offline meeting to occur in order for the abuser to harm the child.

Social Media, including Facebook, Twitter and Instagram: Facebook, Twitter, Instagram and other forms of social media are increasingly becoming an important part of our daily lives, including part of the school's marketing strategy.

- Staff are not permitted to access their personal social media accounts using school equipment at any time, unless granted prior permission by the Headteacher for reasons of work
- Staff are advised not to befriend or follow parents/carers of pupils and to keep their personal profile as private as possible
- Staff and pupils are provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others
- Staff and pupils, are aware that the information, comments, images and video they post online can be viewed by others, copied and stay online forever

Staff and pupils are aware that their online behaviour should at all times be compatible with UK law. Additionally, more information on best practice for staff can be found in our Staff Behaviour (Code of Conduct) Policy.
The Cornwall Independent School recognises that Social media is very likely to play a central role in the fall out from any incident or alleged incident. There is the potential for contact between victim and alleged perpetrator and a very high likelihood that friends from either side could well harass the victim or alleged perpetrator online.

Use of Email:

- Pupils in KS3 and above will be provided with individual email addresses for educational use.
- The use of personal email accounts to send and receive personal data or information is prohibited.
- No sensitive personal data shall be sent to any other young persons, staff or third parties via works email.
- Young people are made aware that all email messages are monitored, and that the filtering system will detect inappropriate links, viruses, malware and profanity.
- Staff members are aware that their email messages may be monitored.
- Any emails sent by young people to external organisations will be overseen by their teacher/support worker and must be authorised before sending.
- Chain letters, spam and all other emails from unknown sources will be deleted without opening.

Taking and Storing Images of Pupils Including Mobile Phones (See our related documents including Appendix 4): The Cornwall Independent School provides an environment in which pupils, parents/carers and staff are safe from images being recorded and inappropriately used. Upon their initial visit, parents/carers, volunteers and visitors are given information informing them they are not permitted to use mobile phones on the premises in the presence of pupils, or to take photographs of pupils apart from circumstances as outlined in Appendix 6 of this policy. This prevents staff from being distracted from their work with pupils and ensures the safeguarding of pupils from inappropriate use of mobile phone cameras and other digital recording equipment. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images of themselves and others especially on social networking sites.
- Photographs published onto any website will comply with good practice guidance on the use of such images. Care will be taken to ensure that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute. Their full names will not be used anywhere in the website, particularly in association with photographs.

N.B. The word ‘camera’ in this document refers to any device that may be used to take and store a digital image e.g. mobile phone, tablet, laptop etc. The school has a Mobile Phone Policy which includes:

- The commitment to keep the pupils safe.
- How we manage the use of mobile phones at The Cornwall Independent School, taking into consideration staff, pupils on placement, volunteers, other professionals, visitors and parents/carers.
- How we inform parents/carers, visitors and other professionals of our procedures.
- What type of mobile phones will be used on educational visits and learning outside the classroom.
- The consequences of any breaches of this policy.
- Reference to other policies, such as Whistleblowing and Safeguarding Children-Child Protection Policies.

Remote Learning (Please see our Remote Learning Policy for more details): Where there are periods in which the school is forced to close yet continue to provide education (such as during the COVID-19 Pandemic) it is important that The Cornwall Independent School supports staff, pupils and parents/carers to access learning safely, especially considering the safety of our vulnerable pupils. Staff and volunteers are aware that this difficult time potentially puts all children at greater risk and the school recognises the importance of all staff who interact with children, including online, continuing to look out for signs a child may be at risk. Staff and volunteers will continue to be alert to any signs of abuse, or effects on learners’ mental health that are also safeguarding concerns and will act on concerns immediately. Any such concerns should be dealt with as per the Child Protection Policy and where appropriate referrals should still be made to children’s social care and as required, the police. Online teaching should follow the same principles as set out in the school’s staff and pupils respective Behaviour - Code of Conducts. Additionally, school name will ensure any use of online learning tools and systems is in line with privacy and data protection/GDPR requirements.

The school will put additional measures in place to support parents and students who are learning from home. This will include specific guidance on which programmes the school is expecting students to use and how to access these alongside how students and parents can report any concerns that they may have. Guidance will also be issued on which staff members students will have contact with and how this will happen, including how to conduct virtual lessons (including video conferencing). Details of this can be found in our schools Remote Learning Policy.

Additionally, the Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, with the day-to-day responsibility being delegated to the Online Safety Officer who is our DSL. The Headteacher works alongside the DSL and they are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff, which in line with our main safeguarding reporting procedures.

Staff working remotely should wherever possible use their school-issued ICT equipment, however they may use their own computer equipment if this is not practical, as long as it is in accordance with the school’s Data Protection Policy. Staff are responsible for security of personal data and must ensure it is stored securely when using personal systems or remote systems to maintain confidentiality from other members of the household.

For more information relating to Online Safety procedures, refer to the Online Safety Frequently Asked Questions (FAQ) in Appendix 5. It covers the following topics on the relevant page as follows:

1 How will the policy be introduced to pupils? How will staff be consulted and made aware of this policy? How will complaints regarding Internet use be handled? How will parents/carers' support be enlisted?
2 Why is the use of Internet and ICT important? How is the safe use of ICT and the Internet promoted? How does the Internet and use of ICT benefit education in our school? How will pupils learn to evaluate Internet content?
3 How is filtering managed? How are emerging technologies managed? How to react to misuse by pupils and young people
4 How is printing managed? What are the categories of Cyber-Bullying? What are the pupil rules?
5 What has research into Cyber Bullying found? What is the impact on a child of ICT-based sexual abuse? What is the impact on a child of ICT-based sexual abuse? How do I stay secure on the Internet? Why is promoting safe use of ICT important? What does the school's Mobile Phone Policy Include?
6 Where can we learn more about Prevent? What do we have to do?
7 Do we have to have a separate *Prevent* Policy? What IT filtering systems must we have? What is the definition of a visiting speaker? Do we have to check all our visiting speakers? What checks must we run on visiting speakers? What do we have to record in our Single Central Register about visiting speakers?
8 What training must we have? What are the potential legal consequences if we do not take the *Prevent* duty seriously? What are the rules for publishing content online?

Related documents:

- Online Safety Appendices 1-6
- Safeguarding Children- Child Protection Policy; Sexual Violence and Sexual Harassment (Including Peer-on-Peer Abuse Policy); Anti-Bullying Policy; Behaviour and Discipline Policy; Staff Behaviour (Code of Conduct) Policy.
- Prevent Duty: Tackling Extremism and Radicalisation Policy; Spiritual, Moral, Social and Cultural Development (SMSC); Personal; Personal Social, Health, Economic Education (PSHEE); The School Rules.
- Mobile and Smart Technology Policy, including taking and storing images of pupils; Acceptable use of ICT Sign off forms for Staff/Pupils; Use of Photographs Sign-off Form.

Legislation and guidance:

- Part 3, paragraphs 7 (a) and (b) of the Education (Independent School Standards) (England) Regulations 2014, in force from the 5th January 2015 and as amended in September 2015
- Keeping Students Safe in Education (KCSIE) Information for all schools and colleges (DfE: September 2022) incorporates the additional statutory guidance,
- Disqualification under the Childcare Act 2006 Childcare (Disqualification) and Childcare (Early Years Provision Free of Charge) (Extended Entitlement) (Amendment) Regulations 2018.
- Working Together to Safeguard Students (WT) (HM Government: September 2018) which also refers to non-statutory advice, Information sharing HM Government: March 2015); Prevent Duty Guidance: for England and Wales (March 2015) (Prevent). Prevent is supplemented by The Prevent duty: Departmental advice for schools and childminders (June 2015) and The use of social media for on-line radicalisation (July 2015) How Social Media Is Used To Encourage Travel To Syria And Iraq: Briefing Note For Schools (DfE)
- Based on guidance from the DfE (2014) 'Cyberbullying: Advice for Heads and School staff 'and 'Advice for parents and carers on cyberbullying'
- Prepared with reference to DfE Guidance (2014) Preventing and Tackling Bullying: Advice for school leaders and governors and the relevant aspects of Safe to Learn, embedding anti-bullying work in schools.
- Having regard for the guidance set out in the DfE (Don't Suffer in Silence booklet)
- The Data Protection Act 1998; GDPR, 2018; BECTA and CEOP.
- Teaching Online Safety in School (DfE: 2019)
- The policy also takes into account the National Curriculum computing programmes of study.
- Meeting digital and technology standards in Schools and Colleges (DfE: 2023) (including Broadband, Cyber-Security and data protection procedures)
- Filtering and monitoring standards for schools and colleges (DfE: 2023)
- Promoting and supporting mental health and wellbeing in schools and colleges (September 2022)
- Behaviour in schools (September 2022)
- Education for a connected world (2020)

- Harmful Online challenges and online hoaxes (2021)

Guidance (UK Safer Internet Centre)

- 2023 Appropriate filtering and monitoring definitions published (UK Safer Internet Centre)
- Test Your Internet Filter (UKSIC / SWGfL)
- A Guide for education settings and filtering providers (UKCIS)
- Establishing appropriate levels of filtering (UKSIC)
- Online safety in schools and colleges: questions from the governing board (UKCIS)
- Sharing nudes and semi-nudes: advice for education settings working with children and young people

The following legislation and guidance should be considered:

- Data Protection Act 1998
- Human Rights Act 1998
- Regulatory of Investigatory Power Act 2000
- Computer Misuse Act 1990 – Police and Justice Act 2006
- Prevent Duty – Counterterrorism and Security Act 2015
- Obscene Publications Act 1959, Protection of children Act 1988, Criminal Justice Act 1988

Appendix 1 – Pupil and Parent/Carers Acceptable Use Policy

The acceptable use policies below are expected to be read and signed by all pupils. We ask parents/carers to have read and understood the policy to support us with keeping children safe when using devices.

All pupils must follow the rules outlined in this policy when using school ICT resources and equipment, including all Internet access and the Virtual Learning Environment (VLE), accessed from both in and outside of school, and on school-provided or personal electronic devices. Breaking these conditions may lead to: confiscation of any electronic devices, close monitoring of the pupil’s network activity, investigation of the pupil’s past network activity, withdrawal of the pupil’s access and, in some cases, permanent removal from the School and even criminal prosecution. Pupils are also expected to take care of school-issued electronic devices and any damage to them may result in charges to replace or fix damaged devices. Misuse of the Internet will be dealt with in accordance with the school's Behaviour and Discipline Policy and, where there is a safeguarding risk, the Safeguarding & Child Protection Policy. The school is not responsible for any loss of data on the network, computers connected to the network or data storage used on the network (including USB memory sticks). Data held on the network will be backed up for a limited period. Pupils are responsible for backups of any other data held. Use of any information obtained via the network is at the pupil’s own risk.

Pupil Acceptable Use Agreement (EYFS/ KS1)

Think before you click

S

I will only use technology, apps and the internet with the permission of an adult.

A

I will only click on apps, icons and links that I know are safe. If I'm not sure I will ask an adult first.

F

I will be polite and friendly when online.

E

If I see something online that I don't like, upsets or worries me I will tell an adult I trust.

I have discussed and agreed this policy with my child
Name of Child: ________________________________
Year Group: ________________________________
Parent Signature: ________________________________
Date: ________________________________

Pupil Acceptable Use Policy (KS2)

This is how we stay safe when we use technology:

- I understand that I am responsible for my own actions.
- I will use my knowledge of internet safety to guide me whenever and wherever I am online.
- I understand that the school will check my online files and monitor the internet sites I visit.
- I will respect copyright and not copy anyone's work and call it my own.
- I will only edit or delete my own files and not look at, or change, other people's files without their permission.
- I will keep my logins and passwords secret.
- I am aware that some websites and social networks have age restrictions, and I must respect this.
- I will not attempt to visit Internet sites that I know to be filtered by the school.
- The messages I send, or information I upload, will always be polite and sensible.
- I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission.
- I will report any unpleasant material to a teacher immediately because this will help protect other pupils and myself.

I have read and understand these rules and agree to them.

Name of Child: ______________________________

Childs Signature: ______________________________

Class: ______________________________

Parent Signature: ______________________________

Date: ______________________________

Pupil Acceptable Use Policy (KS3/4)

This is how we stay safe when we use technology:

The school provides children with access to resources on the Internet via the World Wide Web and occasional email use. We expect that children will follow the guidelines for use that are laid down in this document.

The following guidelines should be adhered to whenever children are working on the network.

Guidelines for Internet and Local Network Access at The Cornwall Independent School

1. Use of the school network and access to the Internet is governed by the same rules that apply in any other part of the school. This includes general behaviour and respect for other people and their privacy.
2. Remember that access is a privilege, not a right, and that access requires responsibility.
3. A member of staff must be present when the ICT Suite is in use.
4. Pupils must not use Chat Rooms in school.
5. Access to the World Wide Web is for school use only. This includes class work and topic work. Children are not allowed to seek information of an unsavoury character, i.e. nothing likely to upset anyone. Remember that it is easy to find out where you have been searching on the net. Your 'footprints' leave a trail to be followed.
6. It is easy to lose your way in the mass of information on the World Wide Web. You should plan your use of the Internet carefully and have a specific goal otherwise you will waste time and effort.
7. Pupils are not allowed to use email unless a staff member has sanctioned its use in a specific situation and under supervision.
8. Any files or messages stored or sent on the school system should not be regarded as totally private as they may be viewed by a senior member of staff. The school provides space on the network for you to store your files, but there is limited space, and you should only keep files on the network that are for school use.
9. Everyone should respect the ICT facilities and equipment and should try to do all they can to keep them working efficiently.
10. Food, drink and bags are not allowed in the ICT room.
11. Misuse of the Internet will result in a child's access privileges being withdrawn.
12. Senior pupils are allowed mobile phones for reasons of safe travelling, but they may not use them to access the internet, camera or other functions on the school premises. The phones must be logged in the School Office daily.

Once you have read and understood this document please sign and return one copy and keep the other for your reference.

Miss L Adams
Headteacher

I have read and understood the above and agree to follow these guidelines at all times.

Pupil's Name: **(Please print) Class:**

Pupil's Signature: **Date:**

My child and I have read these guidelines through together and understood them.

Pupil's Name: **(Please print)**

Parent/Guardian's Signature: **Date:**

Appendix 2 – Staff and Volunteer Acceptable Use of ICT Policy:

Staff (and Volunteer) Acceptable Use Policy Agreement

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools/academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This acceptable use policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance opportunities for pupils' learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school digital technology systems are primarily intended for educational use.
- I will not disclose my usernames or passwords to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will be professional in my communications and actions when using school systems:
- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language, and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website/VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any online activity that may compromise my professional responsibilities.

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up-to-date anti-virus software and are free from viruses.
  - I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
  - I will ensure that my data is regularly backed up, in accordance with relevant school policies.

- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will try not (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the data protection policy. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.
- I understand that the data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software; however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this acceptable use policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. In the event of illegal activities, this would include the involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer Name: ---
Signed: ---
Date: ---

Appendix 3 - Mobile and Smart Technology Policy, including taking and storing images of pupils and staff

Legal Status:
Teaching Online Safety in School: DfE 2019
Cyberbullying: Advice of Headteachers and School Staff: DfE, 2014
Department for Education's published guidance

Introduction: Whilst we welcome the use of mobile phones and cameras for educational purposes and the convenience they offer and recognise that learning to use digital technology is an important part of the ICT and wider curriculum, equally we have to ensure the safeguarding needs of the pupils are met and staff, parents/carers and volunteers are not distracted from their care of pupils. Mobile phones, alongside other technologies aim to change the way we communicate. This speed of communication will often provide security and reassurance; however, as with any other form of technology there are associated risks. Pupils and young people must be encouraged to understand such risks, to enable them to develop the appropriate strategies which will keep them safe. Acceptable use and management of mobile phones is therefore to be agreed by all service users. There is to be a clear expectation that the personal use of mobile phones is to be limited to specific times and uses set out within the policy.

Aims: The aim of this Policy is to protect all users from harm, by ensuring the appropriate management and use of mobile phones by all individuals who work or visit our school, including pupils themselves. Pupils and young people are also to be empowered with the skills to manage the changes in technology in a safe and appropriate way; and to be alert to the potential risks of such use. This is to be achieved through balancing protection and potential misuse. It is therefore to be recognised that alongside the potential risks, mobile phones continue to be effective communication tools. This in turn is to contribute to safeguarding practice and protection.

Policy statement: It is to be recognised that it is the enhanced functions of many mobile devices that will give the most cause for concern; and which should be considered the most susceptible to potential misuse. Examples of misuse are to include the taking and distribution of indecent images, exploitation and cyberbullying. It must be understood that should mobile phones be misused, there will be a negative impact on an individual's safety, dignity, privacy and right to confidentiality. Such concerns are not to be considered exclusive to pupils and young people, so the needs and vulnerabilities of all must be respected and protected.

Mobile phones will also cause an unnecessary distraction during the working day and are often to be considered intrusive when used in the company of others. It will often be very difficult to detect when mobile phones are present or being used. The use of all mobile phones needs to be effectively managed to ensure the potential for misuse is to be minimised.

Code of conduct: A code of conduct is to be promoted with the aim of creating an informed workforce, who will work together to safeguard and promote positive outcomes for the pupils and young people in their care. It is to be ensured that all teachers and staff will:

- Be aware of the need to protect pupils from harm.
- Have a clear understanding of what constitutes misuse.
- Know how to minimise risk.
- Be vigilant and alert to potential warning signs of misuse.
- Avoid putting themselves into compromising situations which could be misinterpreted and lead to potential allegations.
- Understand the need for professional boundaries and clear guidance regarding acceptable use.
- Be responsible for the self-moderation of their own behaviours.
- Be aware of the importance of reporting concerns immediately.

Guidance on Use of Mobile Phones by Teaching Staff: The following points apply to all staff and volunteers at our school and apply to the use of all mobile devices to ensure the quality of supervision and care of the pupils, as well as the safeguarding of pupils, staff, parents and volunteers in the school.

The Cornwall Independent School allows staff to bring in mobile phones for their own personal use. However, they must be kept away in closed drawers or their bags when teaching and are not allowed to be used in the presence of pupils. They may be used during working hours in a designated break away from the pupils. Staff are not permitted to use recording equipment on their personal devices to take photos or videos of pupils. If staff fail to follow this guidance, disciplinary action may be taken in accordance to The Cornwall Independent School Disciplinary Policy. During outings, nominated staff will be permitted to have access to their own mobile phones, which are to be used for emergency contact only. During off-campus activities, i.e. field trips and overnight excursions, trip leaders will be provided with a school-issued mobile phone in good working condition. School-issued mobile phones must be switched on and turned to loud to ensure that staff can be contacted by the school. Contact numbers for all members of staff accompanying the pupils must be left at Reception and a list of contact telephone numbers for all pupils should be with the leader of the off-site activity (although these must be kept confidential).

If staff need to make an emergency call, (such as summoning medical help or reporting an intruder on the premises) they must do so irrespective of where they are, via their own mobile phone or a school phone. Staff should provide the school number to members of the family and next of kin so in an emergency the member of staff can be contacted on the school phone. Staff must ensure that there is no inappropriate or illegal content on their phones or mobile devices. Should any member of staff become aware of inappropriate use of a mobile phone, this should be reported to a member of the SLT and may be subject to disciplinary action.

All teachers are responsible for the storage of school mobile devices, which should be locked away securely when not in use. Images taken and stored on school devices should be uploaded to the school's secure network and deleted from the device when no longer required. Staff are not to use their own equipment to take photos of pupils. Under no circumstances must devices of any kind be taken into the pupil toilets (this includes any device with photographic or video capabilities).

Guidance on staff use of social media: Staff must not post anything onto social networking sites such as Facebook that could be construed to have any impact on the School's reputation. (We advise all our staff to carefully restrict their Facebook profiles to ensure they cannot be contacted by parents and pupils; this could involve removing their last name from their page). We explain to staff that although they are able to accept friendship requests from friends, who may also be parents of pupils at the school, staff must be aware of the potential issues this could cause. Staff must not post anything onto social networking sites that would offend any other member of staff or parent. If any of the above points are found to have occurred, then the member of staff involved will face disciplinary action, which could result in dismissal. Where email contact is initiated by pupils who have left The Cornwall Independent School, employees may reply from a school email address only with blind copies to line managers **and** the DSL. Staff must not accept friendship requests from pupils on roll and we advise staff not to accept requests from former pupils.

Guidance on Use of Mobile Devices by Pupils (mobile network access: 3G, 4G, 5G): Dependent on age, some pupils are permitted to have mobile devices whilst on the school grounds. However, the school recognises that by using devices which have access to 3G, 4G and 5G mobile phone networks, this can result in children having unlimited and unrestricted access to the Internet, which could lead to some children, whilst at school or college, sexually harassing their peers via their mobile and smart technology, sharing indecent images: consensually and non-consensually (often via large chat groups), and viewing and sharing pornography and other harmful content. The school takes precautions to ensure that pupils limit access to their personal mobile devices during the school day and reserves the right to confiscate and monitor personal devices when deemed necessary for safeguarding concerns. For pupils in EYFS-KS2, if pupils bring in a mobile device, it should be turned off and be lodged with the school office. For pupils in KS3/KS4, mobile devices should be switched off and kept securely in lockers or in their school bag unless permission has been given by the classroom teacher, such as for use in note taking or data collection. In the event of a mobile phone being used in a lesson without permission from the teacher, the phone should be confiscated and given to the Headteacher.

The School has the right to confiscate and search any mobile electronic device (personal or school-issued) if it suspects that a pupil or staff member is in danger or has misused a device. This will be done in accordance with the School's policy on searching and confiscation as set out in the Behaviour and Discipline Policy.

Unacceptable Uses: In order to protect one's privacy and respect to others, unless express permission is granted, mobile phones, laptops and mobile devices should not be used to make calls, send messages, use the Internet, take photos or use any other application during school lessons, other educational activities such as assemblies, or in The Cornwall Independent School Dining Halls.

- Mobile devices should not disrupt classroom lessons with ring tones, music or beeping. They should be turned off during lesson times in order to respect the learning environment.

- Using mobile devices to intimidate, bully, harass, threaten, attempt to radicalise others or breach copyright laws is unacceptable. Cyber bullying will not be tolerated. In some cases, it can constitute criminal behaviour. If the use of technology humiliates, embarrasses or causes offence it is unacceptable regardless of whether 'consent' was given. (Please refer to our Anti-bullying Policy)
- Mobile phones are not to be used in changing rooms or toilets or used in any situation that may cause embarrassment or discomfort to their fellow pupils, staff or visitors to the school.
- Disruption to lessons caused by a mobile phone or any mobile device may lead to disciplinary consequences.
- Any pupil who uses vulgar, derogatory, or obscene language while using a mobile phone may face disciplinary action.
- Safeguarding, privacy and respect are paramount at The Cornwall Independent School. To this end, it is prohibited to take a picture of or record a member of staff without their permission. In the event that this happens the pupil will be asked and expected to delete those images and may be requested to turn over the device to the Headteacher and/or the Designated Safeguarding Lead.
- For safety reasons, headphones/earphones should not be used whilst moving around campus during the school day, whilst waiting for or during lessons and assemblies, or in The Cornwall Independent School dining halls
- Pupils are reminded that 'sexting' (sending or posting images or videos of a sexual or indecent nature) is strictly prohibited by the school and may constitute a criminal offence. Pupils must ensure that files stored on their phones do not contain violent, degrading, racist or pornographic images. The school will treat incidences of sexting (both sending and receiving) as a safeguarding issue and pupils concerned about images that they have received, sent or forwarded should speak to any member of staff for advice.

This may result in disconnection from the school network, confiscation of the mobile technology and/or legal or civil disciplinary action. Uploading images and sound is only permissible if the subject involved gives permission and if in doing so, School and statutory guidelines are not breached.

Additionally, 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. When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the School rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL, Prevent lead
or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of a School discipline), and/or
- Report it to the police

Theft or damage: Mobile phones or any mobile devices that are found in the school and whose owner cannot be located should be handed to the front office reception. The school accepts no responsibility for replacing lost, stolen or damaged devices. The school accepts no responsibility for damage to or loss of mobile phones or mobile devices while travelling to and from school. **It is strongly advised that pupils use passwords/pin numbers to ensure that unauthorised phone calls cannot be made on their phones or other mobile devices. Pupils must keep their password/pin numbers confidential.**

Inappropriate conduct in exams: Under exam regulations, mobile phones are prohibited from all examinations. Pupils MUST give phones to invigilators before entering the exam hall. Any pupil found in possession of a mobile phone during an examination will have that paper disqualified. Such an incident may result in all other exam papers being disqualified.

Use of images: displays etc

We will only use images of our pupils for the following purposes:

- Internal displays (including clips of moving images and yearbooks) on digital and conventional notice boards within School premises.
- Communications with The Cornwall Independent School community (parents, pupils, staff), for example newsletters and E-learning Journals.

- Marketing The Cornwall Independent School, both digitally by website, by prospectus [which includes a DVD and YouTube channel], by displays at educational fairs and other marketing functions [both inside the UK and overseas] and by other means.

Storage and Review of Images: Images of pupils should be stored securely on the school network. Digital photographs and videos are reviewed annually and are deleted when no longer required. We regularly check and update our web site, with expired material deleted.

The Cornwall Independent School Website and Social Media Pages: Photographs and videos may only be uploaded to the school's website or social media accounts with the Headteacher's approval. Pupil's surnames are never used on our website or social media pages.

Images that we use in displays and on our web site: The images that we use for displays and communications purposes never identify an individual pupil. Instead, they name the event, the term and year that the photograph was taken (for example, 'Sports Day, Summer Term 2019'). We only use images of school activities, such as plays, concerts, sporting fixtures, prize-giving, school trips etc. in their proper context. We never use any image that might embarrass or humiliate a pupil. Pupils are always properly supervised when professional photographers visit The Cornwall Independent School. Parents are given the opportunity to purchase copies of these photographs.

External Photographers: Professional photographs are taken throughout the year at school shows, by local media and Professional School Portraits. The Headteacher ensures that professional photographers are DBS checked and that they have their own stringent regulations, which ensure safeguarding of pupils from inappropriate use of images.

Media coverage: We will always aim to notify parents in advance when we expect the press to attend an event in which our pupils are participating, and we will make every effort to ensure that images including pupils whose parents or guardians have refused permission for such images of their pupils to be used are not used. We will always complain to the Press Complaints Council (PCC) if the media fails to follow the appropriate code of practice for the protection of young people, including the pupils of celebrities.

Staff induction: All new teaching and office staff are given guidance on the school's policy on taking, using and storing images of pupils.

Parents/Visitors and Volunteers use of mobile phones/cameras within the school buildings (Including Photographing Pupils: Parents must ensure mobile phones/cameras are not on display (switched off or silent mode) while in the presence of pupils or in public areas of the school such as during meetings and school events. If staff observe that parents are using their mobile phones whilst in school, we will politely remind visitors as to why we do not permit the use of mobile phones in and around the school. The exception to this would be at an organised event. Staff should remind parents regularly of school policy with regard to mobile phone use with the following statement on weekly emails, when announcing events: "You are welcome to photograph your child at this event providing the images are for personal use only (e.g. a family album) and so are exempt from data protection Laws. Please be aware these images (which may include other pupils) must not be shared on social networking sites or other web-based forums since we regard this as 'making the image public'. Sharing images, or uploading them into a 'public space', is likely to be in breach of data protection." If they wish to make or take an emergency call, they may use the office and the school phone.

The school records images of pupils, both through moving pictures and stills, for assessment and reporting of progress, as well as celebration of their activities. It goes to some lengths to photograph events and performances, which are available on request (or through purchasing), particularly in order to avoid distraction of pupils while performing and disturbance within the audience. Parents are welcome to take photographs of their own pupils taking part in sporting and outdoor events. When an event is held indoors, such as a play or a concert, parents should be mindful of the need to use their cameras and recording devices with consideration and courtesy for the comfort of others. Flash photography can disturb others in the audience, or even cause distress for those with medical conditions; we therefore ask that it is not used at indoor events. Parents are also reminded that copyright issues may prevent us from permitting the filming or recording of some plays and concerts. We always print a reminder in the programme of events where issues of copyright apply. Additionally, the school records images of pupils, both through moving pictures and stills, for assessment and reporting of progress, as well as celebration of their activities. It goes to some lengths to photograph professionally events and performances, which are available on request (or through purchasing), particularly in order to avoid distraction of pupils while performing and disturbance within the audience.

When pupils join The Cornwall Independent School, we ask parents to sign consent for photographs and videos to be taken for such purposes. If consent is withheld, this must be made clear when the consent form is returned to school so that photographs/videos are not published of the individual child concerned. The pupils take part in various events throughout the year, such as assemblies, sporting events, drama and musical productions, field trips, the international festival, etc. Parents are welcome to take photographs of these memorable events, which may include groups of pupils. If a child takes part in the events, the parents are consenting to their child possibly being photographed or included in a group photograph by other parents. Wherever possible, parents who take photographs of groups of children who are in the care of the school should gain consent first, ensuring that once any photographs are taken, they are stored safely and not posted to social media. The school recognises that it cannot police parents taking photographs of pupils who are outside school grounds and not in the school's care, however posting such pictures online may be in breach of data protection laws without consent of all people within the photograph.

Other mobile technology: At The Cornwall Independent School, we recognise the value of mobile technology within our curriculum and our pupils' accommodation. Within the upper school, pupils are required to bring their own devices to support their studies. Any personal device that pupils bring to the school must be used appropriately in line with the Pupils' Acceptable Use Policy and must be kept securely. Where a pupil is found to be misusing a school or personal device, or accessing inappropriate content, the device may be confiscated by the school and appropriate action taken. When accessing the school Wi-Fi, staff and pupils must adhere to their ICT Acceptable Use Policy. Staff, pupils, volunteers and parents are responsible for their own mobile devices and the school is not responsible for theft, loss, or damage.

Appendix 4 – Use of photographs of pupils and data protection form (to be completed by all new parents)

THE USE OF IMAGES OF CHILDREN

There are sometimes occasions when we wish to take photographs or make video recordings of pupils at our school. Sometimes this is for strictly educational purposes and on other occasions it may be for other purposes ancillary to the running of the school (e.g. taking photographs for use in the school's brochure and on the school's web site)

Similarly, there are occasions when the local press visit our school to record particular school events (e.g. school productions) and they may wish to publish photographs of children in newspapers or use recordings of the children on television when reporting these events. In order to comply with the Data Protection Act 1998, the school needs your consent before taking photographs or making video recordings of your child for purposes which are not part of its core activities. We should therefore be grateful if you could answer the following questions, sign and date the form and return it to the school as soon as possible. Failure to make a return will be interpreted as approval.

Name of pupil: **Please delete as appropriate**

1. I agree that the school can take photographs of my child which may be used in school literature (e.g. school's newsletters; the school's brochure and other promotional material etc) **YES / NO**

2. I agree that the school can use images of my child on its website. (Please note that the website can be viewed across the world). **YES / NO**

3. I agree that the school can use images of my child in video recordings to promote the school. **YES / NO**

4. I agree that the school can take photographs and make video recordings of my child for the school's own records archives and future interest (e.g. photographs of sports teams) **YES / NO**

5. I agree that my child can appear in video recordings or in collections of photographs stored on CD Roms which the school may make of school events and which it may sell to parents of children at the school to raise funds for the benefit of the school. **YES / NO**

6. I am happy for the press to take and use images of my child. **YES / NO**

7. The school may give the press the first name only / first and surname (**please delete as appropriate**) of my child for publishing with the child's photograph in a newspaper or for captioning on television. **YES / NO**

Conditions of Consent

1. The information that you provide on this consent form is valid from the time the school receives this form until the time your child leaves the school. If your circumstances change or you change your mind about any issues addressed in this form, please let the school know immediately.

2. The school will not use any images of your child once your child has left the school without obtaining the parents' specific consent.

3. The school will not itself publish names of pupils with any images of children without prior specific and separate consent from parents.

4. If a pupil is named in any text that the school publishes, a photograph will not be included with the text, unless this is the wish of the pupil and parents.

5. The school will generally avoid publishing close up or individual photographs of pupils. The School's preference is to publish class or group images of pupils.

6. The school will only use images of pupils who are appropriately dressed.

7. The school will not pass to the press the names of any pupils appearing in photographs or recordings that the press wish to publish or broadcast, unless a parent has consented to this.

8. If you agree that the media can take and use images of your child you should note that the media's use of images of children is governed separately by the Data Protection Act, other legislation and industry codes of practice.

I have read and understood the conditions of consent.

Signature of person with parental responsibility: ____

Name (in block capitals): ____**Date:** __________________________

Appendix 5: Online Safety FAQs

How will the policy be disseminated to Pupils?

- Rules for Internet access will be posted in all rooms where computers are used
- Pupils will be informed that Internet use may be monitored
- Instruction in responsible and safe use should precede Internet access
- A module on responsible Internet use will be included in the PSHE programme covering both home and school use.
- Pupils will be informed that network and Internet use may be monitored and appropriately followed up.
- Pupils will be made aware of the acceptable use of technology and sign the school AUP upon enrolment

How will ICT system security be maintained?

- The school ICT systems will be reviewed regularly with regard to security
- Security strategies will be discussed, when necessary, at staff meetings.
- Virus protection will be installed and updated regularly.
- Personal data sent over the Internet will be encrypted or otherwise secured.
- Use of portable media such as USB sticks, SD Cards and Hard Drives to carry work should be kept confidential by staff and not used in public computers.

How will staff be consulted and made aware of this policy?

- All staff must accept the terms of staff AUP before using any IT or Internet resource in school.
- All new staff will be taken through the key parts of this policy as part of their induction.
- All staff including teachers, learning support assistants and support staff will be provided with the School Online Safety policy and have its importance explained as part of the child protection training requirement.
- Staff will be informed that network and Internet traffic can be monitored and traced to the individual user.
- Staff development in safe and responsible Internet use, and on the school Internet policy will be provided as required.
- Breaching this Online Safety policy may result in disciplinary action being taken and access to ICT being restricted or removed.
- Staff will read the Acceptable Use Policy and sign the form prior to using school ICT equipment in the school

How will complaints regarding Internet use be handled?

- Complaints of Internet misuse will be dealt with by the Headteacher.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with our Safeguarding & Child Protection Policy and procedures.
- Pupils and parents will be informed of the complaint procedure which is available on The Cornwall Independent School website.
- Parents and Pupils will need to work in partnership with staff to resolve issues.
- There may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.

How will parents' support be enlisted?

- Parents' attention can be drawn to the AUP in newsletters, the VLE and on the school website.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- A partnership approach will be encouraged with parents and could include information booklets, practical sessions and suggestions for safe Internet use at home.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.
- We will maintain a list of Online Safety resources for parents.
- Parents will be invited to attend an Online Safety workshop annually.

Why is the use of Internet and ICT important? Not only is familiarity with the use of ICT equipment a core requirement, but the efficient use of the equipment and available resources is also considered key – for example, the use of email for efficient communication and the correct use of the Internet for research. Staff across the school are making increased use of ICT, which benefits not only the quality of teaching and support services but also their professional development. It is equally important that staff are properly equipped and supported to make the most efficient use of ICT resources. In particular, ICT is extremely beneficial in engaging our pupils, who have learning and physical disabilities. It can also help them to access parts of the curriculum, which they might not otherwise be able to engage with.

All pupils deserve the opportunity to achieve their full potential; in our modern society this should incorporate the use of "Appropriate and Safe" ICT facilities including online resources and services. Internet use is a part of the statutory curriculum and a necessary tool for staff and Pupils. The school has a duty to provide Pupils with quality Internet access as part of their learning experience. In order for the school to maintain such an environment for learners (pupils and adults) everybody must be aware of the need to ensure online protection (Online Safety) and subsequently understand the principles of this policy and the expectations of school practice as documented below.

How is the Safe Use of ICT and the Internet Promoted? The Cornwall Independent School takes very seriously the importance of teaching pupils (and staff) to use ICT - and especially the Internet - in a safe and responsible manner. This will have a positive impact on not only the use of ICT in school, but also outside school in the wider community. The Cornwall Independent School has in place an Internet firewall, Internet content filtering and antivirus software, and various IT security policies, which help to ameliorate the risk of accessing inappropriate and unauthorised material. However, no system is 100% safe and The Cornwall Independent School will further promote safe use of ICT and the Internet by educating pupils and staff about the risks and the ways they can be mitigated by acting sensibly and responsibly. The school will ensure that the use of Internet derived materials by staff and Pupils complies with copyright law. The Cornwall Independent School will help pupils to understand the risks posed by adults or young people, who use the Internet and social media to bully, groom, abuse or radicalise other people, especially pupils, young people and vulnerable adults. Internet safety is integral to the school's ICT curriculum and is also be embedded in our PSHEE and SMSC provision. The latest resources promoted by the DfE can be found at:

- The UK Safer Internet Centre (www.saferInternet.org.uk)
- CEOP's Thinkuknow website (www.thinkuknow.co.uk)
- PSHE Association (https://www.pshe-association.org.uk/)
- Google Legends (KS2) (https://beInternetlegends.withgoogle.com/en_uk)

How does the Internet and use of ICT benefit education in our school?

- Pupils learn effective ways to use ICT and the Internet including safe and responsible use.
- Access to worldwide educational resources including museums and art galleries.
- Educational and cultural exchanges between Pupils worldwide.
- Access to experts in many fields for pupils and staff.
- Staff professional development through access to national developments, educational materials and good curriculum practice.
- Communication with support services, professional associations and colleagues.
- Improved access to technical support.
- Exchange of curriculum and administration data with LA and DfE
- Support of the wider curriculum through the use of word processing, spreadsheet and presentation tools, specialist applications, and the use of the Internet for research purposes.

How will Pupils learn to evaluate Internet content?

- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, evaluation and retrieval.
- Pupils will be taught what Internet use is acceptable and what is not and given clear guidelines for Internet use.
- If staff or Pupils discover unsuitable sites, the URL (address) and content must be reported to the teacher, Online Safety Officer or IT Department.
- Staff and Pupils should ensure that their use of Internet derived materials complies with copyright law

- Pupils will be taught the SIFT Model to be critically aware of the materials they read and show how to validate information before accepting its accuracy.
- Pupils will be taught to acknowledge the source of information used and to respect copyright.

How is Filtering Managed? Having Internet access enables pupils to explore thousands of global libraries, databases and bulletin boards. They are also able to exchange messages with other learners and teachers throughout the world. All unsuitable websites will be filtered and automatically blocked by our security systems and will not be made accessible to pupils. In addition, pupils' usage of our network will be continuously monitored and repeated attempts to access unsuitable sites will alert our IT Department. The IT Department will tailor the filtering to suit the individual needs of subjects and the school generally appropriate to the age of pupils. Although this filtering uses the latest security technology, parents/guardians will wish to be aware that some pupils may find ways to access material that is inaccurate, defamatory, illegal or potentially offensive to some people.

However, at The Cornwall Independent School we believe that the benefits to pupils having access to the Internet in the form of information, resources and opportunities for collaboration exceed any disadvantages. However, as with any other area, parents and guardians of minors along with The Cornwall Independent School share the responsibility for setting and conveying the standards that pupils should follow when accessing and using these media information sources at school and/or at home. During school time, teachers will guide pupils towards appropriate material on the Internet. Outside school, families bear the same responsibility for guidance as they exercise with other information, sources such as television, telephones, films and radio.

- The school will work in partnership with parents/guardians, the Local Authority (LA) and Department for Education (DfE) to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils come across unsuitable on-line materials, they must report it to the DSL/Headteacher immediately.
- The school will take every step to ensure that appropriate filtering systems are in place to protect pupils from unsuitable material and the methods used will be reviewed regularly.
- Any material that the school believes is illegal must be referred to the Internet Watch Foundation (www.iwf.co.uk).

How are Emerging Technologies Managed? ICT has an all-encompassing role within the lives of pupils and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by pupils may include:

- The Internet
- E-mail
- Instant messaging / video messaging apps (WhatsApp / WeChat / iMessage)
- Social media sites (Facebook, Instagram, Twitter, TikTok)
- Blogs (an on-line interactive diary)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Video broadcasting sites (Popular: http://www.youtube.com/ ,Twitch)
- Chat Rooms (Popular www.teenchat.com, Discord)
- Gaming Sites
- Music download sites (Popular Apple, Spotify,)
- Smart Phones (where all of the above can be accessed)
- Mobile technology (e.g. games consoles)

How to React to Misuse by Pupils and Young People

• **Step 1:** Should it be considered that a child or young person has deliberately misused ICT, a letter will be sent to the parent or carer outlining the issue. The child or young person may be temporarily suspended from a particular activity.

• **Step 2:** If there are to be further incidents of misuse, the child or young person will be suspended from using the Internet or other relevant technology for an increased period of time. The parent or carer will be invited to discuss the incident in more detail with a member of the Leadership Team and the most appropriate course of action will be agreed.

• **Step 3:** The sanctions for misuse can be escalated at any stage, should it be considered necessary. In the event that misuse is deemed to be of a serious nature, steps 1 and 2 can be omitted. Should a child or young person be considered to be at risk of significant harm, the Safeguarding & Child Protection Policy must also be applied. Allegations of serious misuse will be reported to the most appropriate agency, for example, the Police or Children's Social Care.

In the event that a child or young person should accidentally access inappropriate material, it must be reported to an adult immediately. Appropriate action is to be taken to hide or minimise the window. The computer will not be switched off nor will the page be closed, as it may be necessary to refer to the site during investigations to allow effective filters to be put in place to prevent further inadvertent access.

How is Printing Managed? The use of the ICT printers may be monitored on an individual basis to encourage careful use of printing resources. As well as being a significant capital cost, the consumables (ink, laser printer toner and drums, and paper) associated with printing represent one of the most expensive ongoing costs associated with ICT. Whilst the school would not wish to discourage the proper use of printers, it is important to ensure that printing facilities are used efficiently and effectively. Pupils and staff are asked to take care not to waste printing resources, for example by using "Print Preview" to check work before sending it to the printer and by using colour print only when necessary.

What are the categories of Cyber-Bullying? Seven categories of cyber-bullying have been identified:

- **Text message bullying** involves sending unwelcome texts that are threatening or cause discomfort;
- **Picture/video-clip bullying via mobile phone cameras** is used to make the person being bullied feel threatened or embarrassed, with images usually sent to other people. 'Happy slapping' involves filming and sharing physical attacks;
- **Phone call bullying via mobile phone** uses silent calls or abusive messages. Sometimes the bullied person's phone is stolen and used to harass others, who then think the phone owner is responsible. As with all mobile phone bullying, the perpetrators often disguise their numbers, sometimes using someone else's phone to avoid being identified;
- **Email bullying** uses email to send bullying or threatening messages, often using a pseudonym for anonymity or using someone else's name to pin the blame on them.
- **Online grooming, Chat room and Social Networking Site abuse** involves sending menacing or upsetting responses to pupils or young people or posting inappropriate material in a public digital locale.
- **Bullying through instant messaging (IM)** is an Internet-based form of bullying where pupils and young people are sent unpleasant messages as they conduct real-time conversations online.
- **Bullying via websites** includes the use of defamatory blogs (web logs), personal websites and online personal polling sites. There has also been a significant increase in social networking sites for young people, which can provide new opportunities for cyber-bullying.

General Housekeeping: The ICT equipment used by the school represents a considerable financial investment. It makes sense to treat it well so that it will remain in good working order. In addition, the ICT resource is finite e.g. computers can run out of disk space; users should be encouraged to think about the amount of file storage they use and the need to keep it well organised. The school does not currently operate a quota system for disk space or mailboxes but will consider doing so should the need arise.
The following will apply:

- Treat ICT equipment with respect and keep areas around ICT equipment clean and tidy.
- Normal school rules and consideration of others applies.
- Keep the amount of storage you use to a minimum. Clear out old and unused files regularly.

Pupil Rules when using school ICT: Due to the variety of resources throughout the school, including the use of portable digital equipment, the following rules are to be considered as appropriate to the location and the resource.

- Obtain permission to access school-issued ICT resources.
- Food and drink must not be consumed near any computer equipment anywhere in the school.
- Any person found defacing or wilfully damaging ICT equipment will be required to correct the damage caused or pay for replacement.
- Computer/device faults should be promptly reported to the ICT Co-ordinator. Please do not attempt to repair them yourself.
- Be aware of correct posture. Always ensure that your chair is at the optimum height for you and that you are sitting correctly at a workstation when possible.
- <u>At the end of a session using an computer station</u>:

- Log off/shut down according to instructions.
- Replace laptops/equipment as directed.
- Wind up and put away any headsets.

What has Research into Cyber Bullying Found? Because of the anonymity that new communications technologies offer, anyone with a mobile phone or Internet connection can be a target for cyber-bullying. Furthermore, bullies can reach much larger numbers within a peer group than they can with conventional bullying. Vindictive comments posted on a website, for instance, can be seen by a large audience, as can video clips sent by mobile phone. Most cyber-bullying is done by pupils in the same class or year group and although it leaves no visible scars, cyber-bullying of all types can be extremely destructive.

- Between a fifth and a quarter of pupils have been cyber-bullied at least once over the previous few months.
- Phone calls, text messages and email are the most common forms of cyber-bullying.
- There is more cyber-bullying outside school than in.
- Girls are more likely than boys to be involved in cyber-bullying in school, usually by phone.
- For boys, text messaging is the most usual form of cyber-bullying, followed by picture/video clip or website bullying.
- Picture/video clip and phone call bullying are perceived as the most harmful forms of cyber-bullying.
- Website and text bullying are equated in impact to other forms of bullying.
- Around a third of those being cyber-bullied tell no one about the bullying.

What is the impact on a child of ICT based sexual abuse? The impact on a child of ICT based sexual abuse is similar to that for all sexually abused pupils. However, it has an additional dimension in that there is a visual record of the abuse. ICT based sexual abuse of a child constitutes significant harm through sexual and emotional abuse. Recognition and response is recognising a situation where a child is suffering, or is likely to suffer a degree of physical, sexual and/or emotional harm (through abuse or neglect) which is so harmful that there needs to be compulsory intervention by child protection agencies into the life of the child and their family.

Why is Promoting Safe Use of ICT Important? The Cornwall Independent School takes very seriously the importance of teaching pupils (and staff) to use ICT - and especially the Internet - in a safe and responsible manner. This will have a positive impact on not only the use of ICT in school, but also outside school in the wider community.

What does the school's Mobile Phone Policy Include?

- The commitment to keep the pupils safe.
- How we manage the use of mobile phones at The Cornwall Independent School taking into consideration staff, pupils on placement, volunteers, other professionals, Proprietor, visitors and parents/carers.
- How we inform parents/carers, visitors and other professional of our procedures.
- What type of mobile phones will be used on educational visits and learning outside the classroom.
- The consequences of any breaches of this policy.
- Reference to other policies, such as Whistleblowing and Safeguarding Children-Child Protection Policies.

What are the rules for publishing content online?

- Staff or Pupil personal contact information will not be published on the school website. The only contact details given on our website will be the school address and telephone number.
- Pupil's full names will not be used anywhere on the school website or other on-line space.
- We may use photographs of pupils or their work when communicating with parents and the wider community, in newsletters and in the school prospectus.
- Photographs will be checked to ensure that they are suitable (photos of pupils in swimwear would be unsuitable).