The Island Learning Trust

Acceptable Use Policy

(including remote & online learning)

Date written: July 2026

Date of next review: July 2027

Acceptable Use Policy: Staff, Trustee's, Volunteers and Pupils

This policy should be read in conjunction with:

- Safeguarding and Child Protection Policy
- Anti-bullying Policy
- Social Media Policy
- Mobile and Smart Technology Policy
- Staff and Adult Behaviour Policy (Code of Conduct)
- AI Policy

Introduction
New technologies have become integral to the lives of children and young people in today's society, both within schools 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.

Safe use of technology is a critical safeguarding responsibility. The Trust recognises that online activity can present risks to children, including exposure to harmful content, online grooming, exploitation, child-on-child abuse, bullying and extremism.

This policy forms part of the Trust's wider safeguarding framework and supports the prevention, identification and response to safeguarding concerns linked to technology use.

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.

Online risks may include:

- Online grooming and exploitation
- Child-on-child abuse, including sexual harassment
- Exposure to harmful or extremist content
- Cyberbullying
- Coercion, control and online manipulation

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

The implementation of this policy is the responsibility of all members of staff.

Roles and responsibilities:
Online Safety is recognised as an essential aspect of strategic leadership at The Island Learning Trust and the Head of School, with the support of Trustee's and the Director of Safeguarding, aims to embed safe practices into the culture of all schools within the trust.

The Trust Board receives regular reports on online safety, filtering and monitoring and provides strategic oversight and challenge. The Safeguarding Trustee holds specific responsibility for oversight of online safety, including the effectiveness of filtering and monitoring systems.

The Head of School ensures that the policy is implemented and compliance with the policy monitored. All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following

school online procedures. Central to this is fostering a 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials.

All staff are responsible for understanding their role in online safety, including awareness of filtering and monitoring systems and how to report concerns.

Pupils use of IT:
Pupils will review our AUP (Appendix 2) with their class teacher annually, with the teacher ensuring that the rules are fully explained and discussed as pupils' individual perceptions of the risks involved may vary. All information will be presented in a manner which is appropriate for the age and stage of the pupils concerned. To support pupils understanding of our AUP, this policy will be sent home annually enabling parents to discuss and support its content. Parents will be asked to sign and return the Parent/Carer Acceptable Use Policy Acknowledgement Form (Appendix 3). Each classroom will display age appropriate Acceptable Use poster so that pupils have a constant frame of reference (Appendix 5 and 6). The Acceptable Use policy will appear regularly on all computers and tablets with pupils and staff needing to click to agree with this policy. In addition to the annual AUP review Online will be taught and embedded across the IT curriculum and will be addressed through curriculum days and themed assemblies.

Children's mobile phones:
Mobile phones are not allowed to be brought into school unless permission has been given by the pupil's class teacher. If a phone is brought into school, it must be switched off when the child enters the school gates and must remained switched off until the child exits the school premises. The phone must immediately be handed into the class teacher or the main office and stored in a secure place until the end of the day. If a learner breaches the school policy, the phone or device will be confiscated and will be held in the school office safe or locked away in a classroom cupboard. Mobile phones and devices that have been confiscated will be released to parents or carers at the end of the school day. If a mobile phone is required for a child due to medical reasons, this must be agreed upon with the Head of School. A care plan must also be in place to ensure the child's needs are clearly understood and appropriately supported.

Filtering and Monitoring:

The Trust ensures that appropriate filtering and monitoring systems are in place to safeguard pupils and staff. Filtering systems block access to harmful and inappropriate content, while monitoring systems identify and flag safeguarding risks.

The Trust ensures that:
- Filtering and monitoring systems are effective, proportionate and regularly reviewed
- Systems are age-appropriate and tailored to the needs of pupils
- Alerts are prioritised according to risk and responded to appropriately
- All staff understand that filtering is not a substitute for supervision

Roles and responsibilities:
- The Director of Safeguarding oversees the effectiveness of filtering and monitoring systems across the Trust
- Designated Safeguarding Leads (DSLs) are responsible for responding to alerts and concerns
- Staff must report any concerns identified through monitoring systems immediately

Each teacher will be responsible for monitoring the use of the internet within their classroom and ensure that unacceptable material is not accessed. The DSL has responsibility for checking that no inappropriate material is on the school system. Staff must not rely solely on filtering systems to manage risk and must remain vigilant when supervising pupils' online activity.

The Trust works with its IT provider to ensure systems meet DfE standards and are regularly tested and reviewed.

Managing the school network:
The computer system / network is owned by the school and is made available to pupils to further their education and to staff to enhance their professional activities including teaching, research, administration and management. The school reserves the right to examine or delete any files that may be held on its

computer system or to monitor any Internet or email activity on the network or perform any other activities that the school may see fit.

Staff, trustee's and volunteers use of IT:
The computers, electronic media and services provided by the school are primarily for educational use to assist staff in the performance of their job and their use must be compliant with the AUP and other associated policies. Limited or incidental use of electronic media for personal purposes is acceptable, and all such use should be done in a manner that does not negatively affect the system's use for their educational purposes. All staff must be aware that their use of technology is subject to monitoring. Staff should understand the types of safeguarding concerns that may be identified through monitoring systems and must report concerns in line with safeguarding procedures. The use of personal devices for professional purposes is discouraged unless explicitly authorised by the Head of School. Where authorised:

- Devices must meet Trust security requirements
- Personal data must not be stored on personal devices
- Only school-approved accounts may be used
- All safeguarding and data protection expectations remain in place

The Island Learning Trust expects any staff using social media sites to ensure that their use is conducive to their professional status. They should not mention the school by name or in passing, or discuss individuals or groups within the school, or compromise the school values. In addition, staff must ensure that any private blogs, bulletin boards, websites etc. which they create, or actively contribute to, do not compromise, and are not confused with, their professional role.

Staff, trustee's and volunteers use of mobile phones:
Staff may have mobile phones in school, but they must be switched off or switched to 'silent' during lesson times. All mobiles and other personal devices must be stored in a safe and secure place during lesson time e.g. locked in a drawer, cupboard or locker. Bluetooth and other forms of communication (such as 'airdrop') are hidden during lesson times. All staff must not accept or make calls during times in classrooms or when working with pupils in other areas of the school. Mobile phones can be taken on all outside visits from the school so that contact with the school is maintained at all times. In these cases, staff need to leave their contact number with appropriate members of staff e.g. Office staff and SLT. Staff must ensure that the use of personal devices does not create safeguarding risks, including the potential for inappropriate communication or blurred professional boundaries.

Parents, carers and visitors use of mobile phones and cameras:
Parents, carers and visitors may have mobile phones in school, but they must be switched off or switched to 'silent' whilst in the school building. Making and receiving calls will be restricted to areas which are free from pupils. Parents and visitors should not take any photographs or video footage of children other than at school events. Any images taken must be for private use only and it should be noted that it is illegal to sell or distribute any such images/recordings without proper permission. Any image/recording shared on social media sites, or the Internet must only be of their own child/ren. The right to withdraw consent will be maintained and any photography or filming on site will be open to scrutiny at all times.

The use of images and video recordings by the school:

General guidance

- Images or videos that include children will be selected carefully when used online.
- Children's' full names will not be used on the website in association with photographs
- The school will not include any personal addresses, emails, telephone numbers, on video, on the website, in a prospectus or in other printed publications.
- The school will only use images of children who are suitably dressed.
- Staff will receive information regarding the safe and appropriate use of images as part of their safeguarding training and responsibilities.
- All members of staff (including volunteers) will ensure that all images are available for scrutiny and will be able to justify any images in their possession.
- Only official setting owned equipment (e.g. work provided digital or video cameras) will be used by staff to capture images of children for official purposes.
- Careful consideration will be given before involving very young or vulnerable children when taking photos or recordings, who may be unable to question why or how activities are taking place.

- The school will discuss the use of images with children and young people in an age appropriate way.
- Images will not be taken of any child or young person against their wishes. A child or young person's right not to be photographed is to be respected.
- Photography is not permitted in sensitive areas such as changing room, toilets, swimming areas etc.
- Photographs will be disposed of should they no longer be required.

Online Communication and Remote Learning:

Online communication and remote learning will be conducted using platforms and systems approved by the Trust. All systems used by schools within the Trust have been assessed and authorised by the Trust Leadership Team.

Staff responsibilities:

- Staff must use school-managed or specifically approved professional accounts when communicating with pupils and/or parents/carers.
- Personal accounts must not be used. Any exceptions due to pre-existing relationships must be discussed with the school's Designated Safeguarding Lead (DSL).
- Where possible, staff should use Trust-provided equipment (e.g. school laptops or mobile devices).
- Online contact must occur only during designated school hours (9:00am – 3:20pm), as defined by the Senior Leadership Team (SLT).
- All remote lessons must be timetabled. Members of SLT, DSL, or Middle Leaders may join sessions at any time.
- Live-streamed sessions require prior approval from the Head of School.

Data protections and security:

- Personal data captured during remote learning will be processed in line with the Trust's data protection policy and with appropriate consent.
- All communication must adhere to school confidentiality standards.
- Only members of the Trust community will be granted access to approved systems.
- Access will be managed in accordance with current IT security protocols.

Session management:

- Staff must record the time, date, duration, and attendance of each session.
- Privacy and safety settings must be used to manage access and interaction, including:
    - Disabling or limiting chat functions.
    - Preventing learners from sharing screens.
    - Keeping meeting IDs private.
    - Using waiting rooms or equivalent features.
- Live contact with learners must occur via school-provided email accounts or parent/carer accounts.
- Staff will control the use of learners' video and microphones, which should be muted during direct instruction.
- At least two staff members should be present during live sessions. If not possible, SLT approval must be obtained.
- One-to-one live sessions require Head of School approval and a parent/carer must be present in the room.
- A pre-agreed invitation/email outlining session expectations must be sent to participants.
- Access links must not be shared publicly or forwarded.
- If sharing is necessary, this must be discussed with the session leader.
- Learners are encouraged to attend sessions in a communal space with an open door and/or appropriate adult supervision.

Behaviour expectations:

- Staff will model safe and respectful behaviour during remote sessions, consistent with classroom standards.
- All participants must follow existing school behaviour policies, including:
    - Using appropriate language.
    - Not recording or capturing images for personal use.
    - Following guidance on whether sessions may be recorded and how recordings may be shared.
- Staff will remind participants of behaviour expectations and reporting procedures at the start of each session.
- Participants must:
    - Wear appropriate clothing.
    - Ensure video backgrounds are neutral.
    - Avoid displaying personal or inappropriate items.
- Educational resources will be shared in accordance with teaching and learning policies, including licensing and copyright requirements.

Reporting concerns:

- Concerns during remote sessions should be reported to the session leader or a parent/carer.
- Inappropriate behaviour or language may result in removal from the session, termination of the session, and reporting to the Head of School.
- Online behaviour issues will be addressed in line with existing policies (e.g. acceptable use, anti-bullying, behaviour, and allegations against staff).
- Sanctions for misuse may include restricted access or police involvement if a criminal offence is suspected.
- Safeguarding concerns will be reported to DSL in accordance with the Trust's safeguarding child protection policy.

Appendix 1

Staff, Visitors and volunteers Acceptable Use Policy:

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

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

Policy Scope

1. I understand that this AUP applies to my use of technology systems and services provided to me or accessed as part of my role within The Island Learning Trust both professionally and personally. This may include use of laptops, mobile phones, tablets, digital cameras and email as well as IT networks, data and data storage and online and offline communication technologies**.**

2. I understand that The Island Learning Trust's Acceptable Use of Technology Policy (AUP) should be read and followed in line with the Staff Code of Conduct.

3. I am aware that this AUP does not provide an exhaustive list; all staff should ensure that technology use is consistent with The Island Learning Trust's ethos, school staff behaviour and safeguarding policies, national and local education and child protection guidance, and the law.

Use of The Island Learning Trust's Devices and Systems

4. I will only use the equipment and internet services provided to me by the school for example school provided laptops, tablets, mobile phones and internet access, when working with learners.

5. I understand that any equipment and internet services provided by my workplace is intended for educational purposes and/or professional use and should only be accessed by members of staff. Reasonable personal use of setting IT systems and/or devices by staff is allowed however personal use is restricted to outside of teaching times.

6. Where I deliver or support remote learning, I will comply with the Trust's remote learning AUP.

Data and System Security

7. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or securing/locking access.
    - I will use a 'strong' password to access school systems. (***A strong password has numbers, letters and symbols, with 8 or more characters).***
    - I will protect the devices in my care from unapproved access or theft e.g. I will not leave the device visible or unsupervised in public places/vehicles.
    - I will complete required cyber security training and follow Trust guidance in line with national standards, including recognising phishing attempts and reporting security concerns immediately.

8. I will respect The Island Learning Trust's system security and will not disclose my password or security information to others.

9. I will not open any hyperlinks or attachments in emails unless they are from a known and trusted source. If I have any concerns about email content sent to me, I will report them to the IT system manager.

10. I will not attempt to install any personally purchased or downloaded software, including browser toolbars, or hardware without permission from the IT system manager.

11. I will ensure that any personal data is kept in accordance with the Data Protection legislation, including GDPR in line with The Island Learning Trust's information security policies.
    - All personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online or accessed remotely.
    - Any data being removed from the school site, such as via email or on memory sticks or CDs, will be suitably protected. This will include the use of encrypted memory sticks and secure emails/storage via Microsoft Office 365.

12. I will not keep documents which contain The Island Learning Trust's related sensitive or personal information, including images, files, videos and emails, on any personal devices, such as laptops,

digital cameras, and mobile phones. Where possible, I will use Microsoft Office 365 to upload any work documents and files in a password protected environment.

13. I will not store any personal information on the school's IT system, including school laptops or similar device issued to members of staff, that is unrelated to school activities, such as personal photographs, files or financial information.

14. I will ensure that school owned information systems are used lawfully and appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

15. I will not attempt to bypass any filtering and/or security systems put in place by the school.

16. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the IT system manager in my setting as soon as possible.

17. If I have lost any school related documents or files, I will report this to the IT system manager and school Data Protection Officer as soon as possible.

18. Any images or videos of learners will only be used as stated in the school's guidance.
    - I understand images of learners must always be appropriate and should only be taken with school provided equipment and taken/published where learners and their parent/carer have given explicit consent.

Classroom Practice

19. I am aware of safe technology use in the classroom and other working spaces, including appropriate supervision of learners, as outlined in the school online safety policy.

20. I have read and understood the school online safety policy which covers expectations for learners regarding mobile technology and social media

21. I will promote online safety with the learners in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create by:
    - exploring online safety principles as part of an embedded and progressive curriculum and reinforcing safe behaviour whenever technology is used on site.
    - creating a safe environment where learners feel comfortable to report concerns and say what they feel, without fear of getting into trouble and/or be judged for talking about something which happened to them online.
    - involving the Designated Safeguarding Lead (DSL) or a deputy as part of planning online safety lessons or activities to ensure support is in place for any learners who may be impacted by the content.
    - make informed decisions to ensure any online safety resources used with learners is appropriate.

22. I will report any filtering breaches (such as access to illegal, inappropriate or harmful material) to the DSL in line with the school's online safety and child protection policies.

23. I will respect copyright and intellectual property rights; I will obtain appropriate permission to use content, and if videos, images, text or music are protected, I will not copy, share or distribute or use them.

24. I am aware that generative artificial intelligence (AI) tools may have many uses which could benefit our school/college community. However, I also recognise that AI tools can also pose risks, including, but not limited to, bullying and harassment, abuse and exploitation (including child sexual abuse), privacy and data protection risks, plagiarism and cheating, and inaccurate, harmful and/or biased material. Additionally, its use can pose moral, ethical and legal concerns if not carefully managed. As such, I understand that:

    - AI tools are only to be used responsibly and ethically, and in line with our trusts safeguarding & child protection, data protection, and professional conduct/behaviour policy expectations.
    - A risk assessment will be undertaken, and written approval will be sought from the senior leadership team prior to any use of AI tools, for example if used in the classroom, or to support lesson planning.
    - A Data Protection Impact Assessment (DPIA) will always be completed prior to any use of AI tools that may be processing any personal, sensitive or confidential data and use will only occur following approval from the DPO.
    - I am required to critically evaluate any AI-generated content for accuracy, bias, and appropriateness before sharing or using it in educational contexts.
    - AI must not be used to replace professional judgement, especially in safeguarding, assessment, or decision-making involving children.
    - Only approved AI platforms may be used with children. Children must be supervised when using AI tools, and I must ensure age-appropriate use and understanding prior to use.
    - Any misuse of AI will be responded to in line with relevant school/trust policies, including but not limited to, anti-bullying, staff and pupil behaviour and safeguarding and child protection.
    - I understand that AI tools may expose users to safeguarding risks, including harmful content, misinformation and inappropriate interactions. Any concerns arising from pupil use of AI will be treated as safeguarding concerns and reported to the DSL

Use of Social Media and Mobile Technology

25. I will ensure that my use of mobile devices and smart technology is compatible with my professional role, does not interfere with my work duties and takes place in line with the staff expanded code of conduct and the law.

    - I will take appropriate steps to protect myself and my reputation online when using communication technology, including the use of social media.
    - I will not discuss or share data or information relating to learners, staff, school business or parents/carers on social media.

26. My electronic communications with current and past learners and parents/carers will be transparent and open to scrutiny and will only take place within clear and explicit professional boundaries.

    - I will ensure that all electronic communications take place in a professional manner via school approved and/or provided communication channels and systems, such as a school email address, user account or telephone number.
    - I will not share any personal contact information or details with learners, such as my personal email address or phone number.

- I will not add or accept friend requests or communications on personal social media with current or past learners and/or their parents/carers.
- If I am approached online by a current or past learner or parents/carer, I will not respond and will report the communication to my line manager and Designated Safeguarding Lead (DSL).
- Any pre-existing relationships or situations that compromise my ability to comply with the AUP will be discussed with the DSL and/or headteacher/head of School.
- I understand that any low-level concerns regarding online conduct, including boundary-blurring behaviour, must be reported in line with the Trust's low-level concerns procedure.

Policy Compliance

27. I will not upload, download, or access any materials which are illegal, such as child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act.

28. I will not attempt to access, create, transmit, display, publish or forward any material or content online that is inappropriate or likely to harass, cause offence, inconvenience, or needless anxiety to any other person.

29. I will not engage in any online activities or behaviour that could compromise my professional responsibilities or bring the reputation of the school into disrepute.

30. I will report and record concerns about the welfare, safety or behaviour of learners or parents/carers to the DSL in line with the school safeguarding and child protection policy.

31. I will report concerns about the welfare, safety, or behaviour of staff to the headteacher/head of school, in line with the allegations against staff policy.

Policy Breaches or Concerns

32. If I have any queries or questions regarding safe and professional practise online either in school or off site, I will raise them with the DSL and/or the headteacher/head of school

33. I understand that the school may exercise its right to monitor the use of its information systems, including internet access and the interception of emails, to monitor policy compliance and to ensure the safety of learners and staff. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.

34. I understand that if the school believe that unauthorised and/or inappropriate use of school systems or devices is taking place, the school may invoke its disciplinary procedures as outlined in the expanded staff code of conduct.

35. I understand that if the school believe that unprofessional or inappropriate online activity, including behaviour which could bring the school into disrepute, is taking place online, the school may invoke its disciplinary procedures as outlined in the expanded staff code of conduct.

36. I understand that if the school suspects criminal offences have occurred, the police will be informed.

Name: _____
Position: _____
Signature: _____
Date: _____

Appendix 2:

Pupil Acceptable Use Policy Key Stage 2 (7-11)

- I understand that the school Acceptable Use Policy will help keep me safe and happy online at home and at school.
- I know that I will be able to use the internet in school for a variety of reasons, if I use it responsibly. However, I understand that if I do not, I may not be allowed to use the internet at school/setting.
- I know that being responsible means that I should not look for bad language, inappropriate images or violent or unsuitable games, and that if I accidently come across any of these I should report it to a teacher or adult in school, or a parent or carer at home.
- I only use websites and search engines that my teacher has chosen.
- I will treat my password like my toothbrush! This means I will not share it with anyone (even my best friend), and I will log off when I have finished using the computer or device.
- I will protect myself by not telling anyone I meet online my address, my telephone number, my school/setting name or by sending a picture of myself without permission from a teacher or other adult.
- I will not arrange to meet anyone I have met online alone in person without talking to a trusted adult.
- If I get unpleasant, rude, or bullying emails or messages, I will report them to a teacher or other adult. I will not delete them straight away, but instead, keep them so I can show them to the person I am reporting it to.
- I will only use AI tools if my teacher says it is safe and appropriate.
- I will always be myself and not pretend to be anyone or anything I am not. I know that posting anonymous messages or pretending to be someone else is not allowed.
- I will always check before I download software or data from the internet. I know that information on the internet may not be reliable, and it sometimes needs checking.
- If I bring in memory sticks/CDs from outside of school/setting, I will always give them to my teacher so they can be checked for viruses and content before opening them.
- I will be polite and sensible when I message people online and I know that sending a message is the same as having a conversation with someone. I will not be rude or hurt someone's feelings online.
- I know that I am not allowed on personal email, social networking sites or instant messaging in school.
- If, for any reason, I need to bring a personal/smart device and/or mobile phone into school I know that it is to be handed in to the class teacher and then collected at the end of the school day.
- I know that all school devices/computers and systems are monitored, including when I am using them at home.
- I will tell a teacher or other adult if someone online makes me feel uncomfortable or worried when I am online using games or other websites or apps.
- I can visit www.ceopeducation.co.uk and www.childline.org.uk to learn more about being safe online or to see help.

Shortened KS2 version (for use on posters)

- I ask a teacher about which websites I can use
- I will not assume information online is true
- I know there are laws that stop me copying online content
- I know I must only open online messages that are safe. If I'm unsure I won't open it without speaking to an adult first
- I know that people online are strangers and they may not always be who they say they are
- If someone online suggests meeting up, I will always talk to an adult straight away
- I will not use technology to be unkind to people
- I will keep information about me and my passwords private
- I always talk to an adult if I see something which makes me feel worried

Pupil Acceptable Use Policy Agreement for younger pupils (Foundation / KS1 0-6)

This is how we stay safe when we use computers/tablets:

- I only use the internet when an adult is with me.
- I only click on links and buttons online when I know what they do.
- I keep my personal information and passwords safe.
- I only send messages online which are polite and friendly.
- I know that the school can see what I am doing online
- I will always tell a teacher or suitable adult if something online makes me feel unhappy or worried. Screen.
- I can visit www.ceopeducation.co.uk, www.childline.org.uk or www.thinkuknow.co.uk to learn more about being safe online or to see help.
- I know that if I break the rules I might not be allowed to use a computer / tablet
- I have read and talked about these rules with my parents/carers

Shortened version (for use on posters)

- I only go online with a grown up
- I am kind online
- I keep information about me safe online
- I tell a grown up if something online makes me unhappy or worried

Appendix 3:
Parent/Carer Acceptable Use Policy Acknowledgement Form

1. I know that my child will be provided with internet access and will use a range of IT systems in in order to access the curriculum and be prepared for modern life whilst at The Island Learning Trust.
2. I am aware that learners use of mobile technology and devices, such as mobile phones, **are only permitted with permission** and that any device allowed onto The Island Learning Trust's premises must be handed in to a member of staff upon entering the school.
3. I am aware that any internet and technology use using The Island Learning Trust's equipment may be monitored for safety and security reasons, to safeguard both my child and The Island Learning Trust's systems. This monitoring will take place in accordance with data protection (including GDPR) and human rights legislation.
4. I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that learners are safe when they use the school internet and systems. I understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.
5. I understand that my child needs a safe and appropriate place to access remote learning. I will ensure my child's access to remote learning is appropriately supervised and any use is in accordance with the Trust's remote learning AUP.
6. I am aware that my child will receive online safety education to help them understand the importance of safe use of technology and the internet, both in and out of school.
7. I have read and discussed The Island Learning Trust's learner Acceptable Use of Technology Policy (AUP) with my child.
8. I will support school safeguarding policies and will ensure that I appropriately monitor my child's use of the internet outside of school and discuss online safety with them when they access technology at home.

9. I know I can seek support from my child's school about online safety, such as via the website, to help keep my child safe online at home.
10. I will support the school approach to online safety. I will role model safe and positive online behaviour for my child by sharing images, text and video online responsibly.
11. I, together with my child, will not deliberately upload or add any images, video, sounds or text that could upset, threaten the safety of or offend any member of the school community.
12. I understand that a partnership approach to online safety is required. If the school has any concerns about either my or my child's behaviour or safety online, then I will be contacted.
13. I understand that if I or my child do not abide by The Island Learning Trust's AUP, appropriate action will be taken. This could include sanctions being applied in line with the school policies including behaviour, online safety and anti-bullying policy and if a criminal offence has been committed, the police being contacted.
14. I know that I can speak to the school's Designated Safeguarding, my child's teacher or the Headteacher/Head of school if I have any concerns about online safety.

I have read, understood and agree to comply with the Acceptable Use Policy.

Child's Name: _____
Child's Class: _____

Parents Name: _____
Parents Signature: _____
Date: _____

Appendix 4:

Dear Parent/Carer

All pupils at The Island Learning Trust use computer facilities and internet access, as an essential part of learning as required by the National Curriculum. Your child will have the opportunity to access a wide range of information and communication technology (IT) resources. This includes access to:

- Computers, laptops and other digital devices
- Internet which may include search engines and educational websites
- Email
- Games consoles and other games based technologies
- Digital cameras, web cams and video cameras

The Island Learning Trust recognises the essential and important contribution that technology plays in promoting children's learning and development, believe it and offers a fantastic range of positive activities and experiences. We do recognise however that this can bring risks. We take your child's online safety seriously and, as such, will take all reasonable precautions, including monitoring and filtering systems, to ensure that pupils are safe when they use our internet and systems.

We recognise however that no technical system can replace online safety education and believe that children themselves have an important role to play in developing responsible behaviour. In order to support the school in developing your child's knowledge and understanding about online safety, we request that you read the attached Acceptable Use Policy with your child, discuss the content with them and return the attached slip.

Hopefully, you will also find this Acceptable Use Policy provides you with an opportunity for conversations between you and your child about safe and appropriate use of the technology, both at school and at home.

We request that all parents support our approach to online safety by role modelling safe and positive online behaviour and by discussing online safety whenever children access technology at home. Parents can visit the school website for more information about the approach to online safety. Full details of the school's online safety policy are available on the school website or on request. Parents/carers may also like to visit the following links for more information about keeping children safe online:

- www.thinkuknow.co.uk
- www.childnet.com

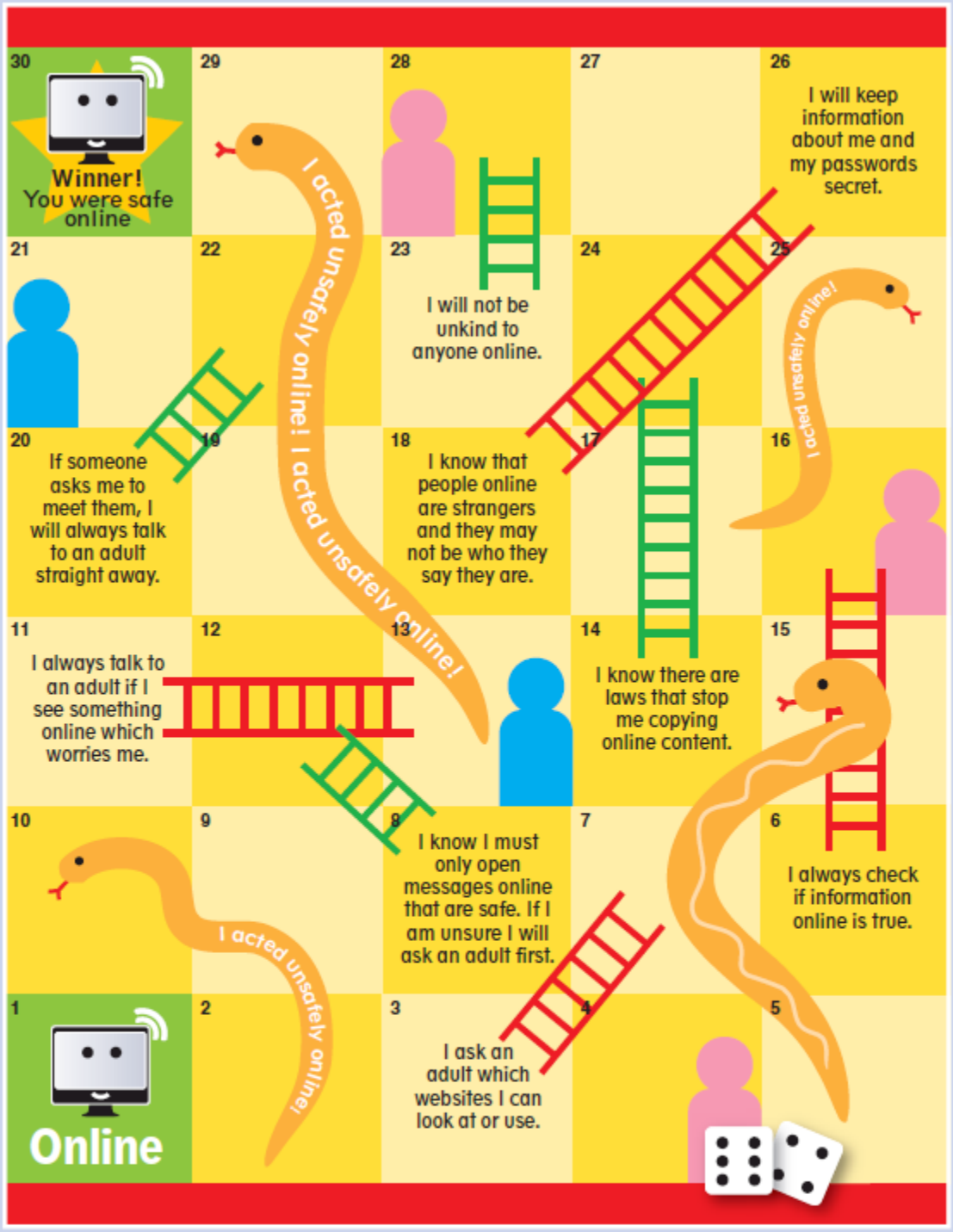
- www.nspcc.org.uk/onlinesafety
- www.saferinternet.org.uk
- www.internetmatters.org
- www.ceopeducation.co.uk

Should you wish to discuss the matter further, please do not hesitate to contact the school Designated Safeguarding Lead or myself.

Yours sincerely,
Headteacher/Head of School

Appendix 5: Early Years and KS1 Acceptable Use Poster

Appendix 6: KS2 Acceptable Use Poster



STAY SAFE Online

eis Kent Education iT Services

Kent County Council kent.gov.uk

Published by EIS Kent • 0300 065 8800 • www.eiskent.co.uk

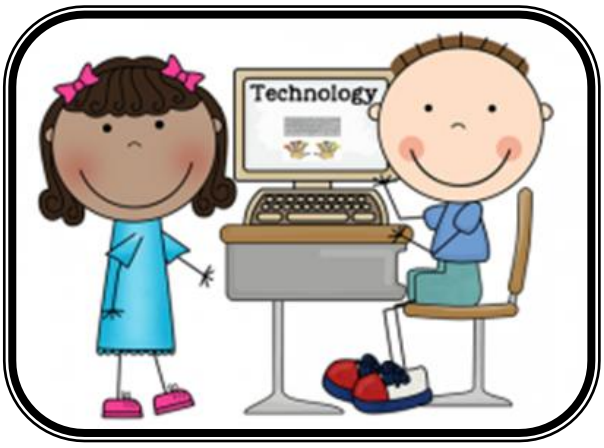
Appendix 7 Online Incident Reporting Log

Online Safety Incident Reporting

Date/time:	
Child and/or Workstation name (If appropriate):	
Incident or concern raised:	
Action Taken:	
Member of staff (please print name):	Signed:
DSL:	Signed:

Appendix 8 Key Stage 1 Online Incident Poster

Online Incidents

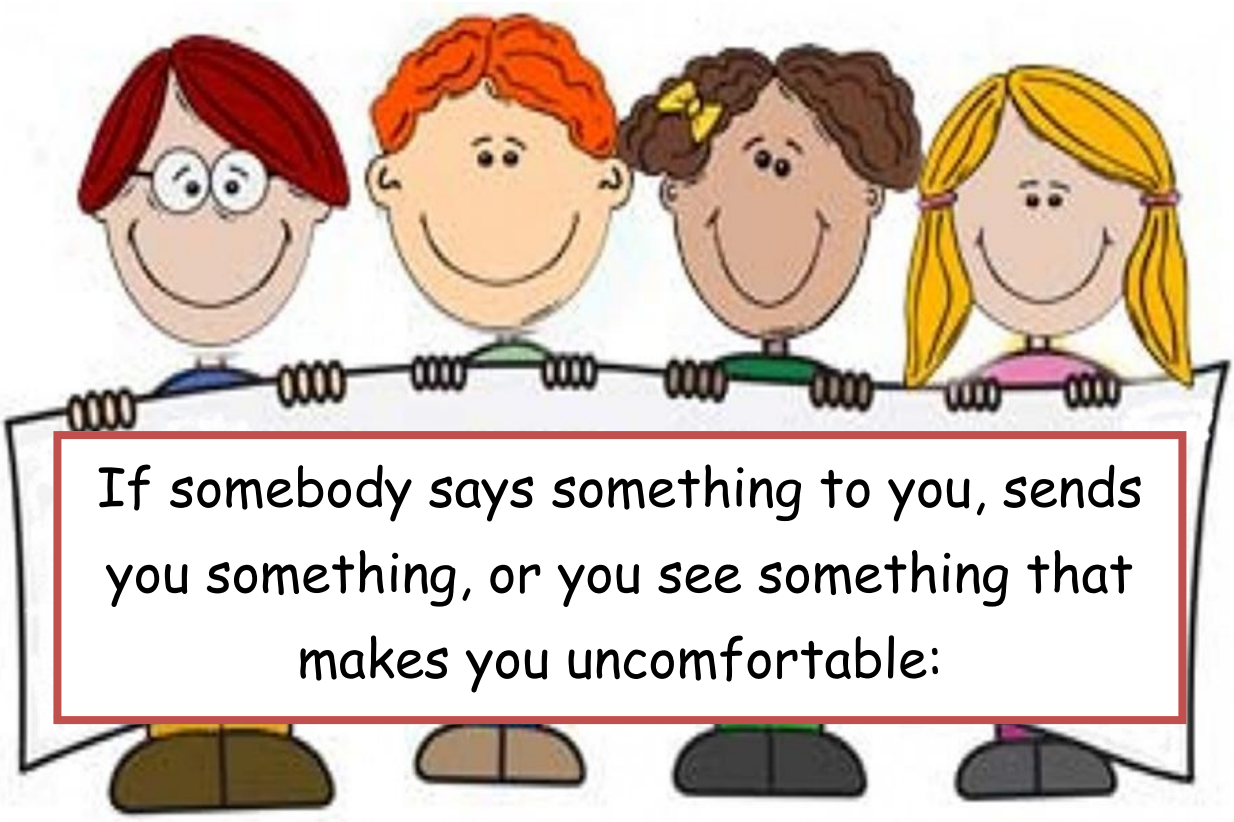


If you see something on the screen that makes you worry or feel sad:

Turn off the monitor

Tell an adult

Online Incidents



If somebody says something to you, sends you something, or you see something that makes you uncomfortable:

Turn off the monitor

Tell an adult

The Island Learning Trust

The Island Learning Trust