The
TILIAN PARTNERSHIP
Inspire to achieve

Online Safety Policy

Cavendish CE Primary School

Approved by:	SGC	**Date:**	25/11/2025
Last reviewed on:	November 2025		
Next review due by:	November 2026		

Aims

This policy aims to explain how parents/carers, children or young people can be a part of these safeguarding procedures. It also details how children and young people are educated to be safe and responsible users capable of making good judgements about what they see, find and use. The term 'Online Safety' is used to encompass the safe use of all technologies in order to protect children, young people and adults from potential and known risks.

- To emphasise the need to educate staff, children and young people about the pros and cons of using new technologies both within and outside school.
- To provide safeguards and agreement for acceptable use to guide all users, whether staff or student, in their online experiences.
- To ensure adults are clear about procedures for misuse of any technologies both within and beyond the school.
- To develop links with parents/carers and the wider community ensuring input into policies and procedures with continued awareness of the benefits and potential issues related to technologies.

Roles and Responsibilities of the Partnership

It is the overall responsibility of the headteacher to ensure that there is an overview of Online Safety as part of the wider remit of safeguarding across the school with responsibilities as follows:

- The Head is responsible for designating the Online Safety Lead.
- The Head will ensure implementation of agreed policies, procedures, staff training, curriculum requirements and taking responsibility for ensuring Online Safety is addressed in order to establish a safe computing learning environment.
- The Head is responsible for promoting Online Safety across the curriculum and has an awareness of how this is being developed.
- School Governance Committees must ensure Online Safety is covered within an awareness of safeguarding and how it is being addressed within the school. It is the responsibility of the SGC to ensure that all safeguarding guidance and practices are embedded.
- The School Governance Committee will ensure that any misuse or incident has been dealt with appropriately, according to policy and procedures, (see the Managing Allegations Procedure on Suffolk Local Safeguarding Children's Board website) and appropriate action is taken, even to the extreme of suspending a member of staff, informing the police (via establishment's agreed protocols with the police) or involving parents/carers.

Online Safety Lead

It is the role of the designated Online Safety Lead to:

- Ensure that filtering is set to the correct level for staff, children and young people.
- Appreciate the importance of Online Safety within school and to recognise that all educational establishments have a general duty of care to ensure the safety of their pupils and staff.
- Establish and maintain a safe computing learning environment within the school.
- Ensure that all adults are aware of the filtering levels and why they are there to protect children and young people.
- Report issues and update the Headteacher on a regular basis.
- Update staff training (all staff) according to new and emerging technologies so that the correct Online Safety information can be taught or adhered to.
- Take joint responsibility with the Headteacher to keep a log of incidents for analysis to help inform future development and safeguarding, where risks can be identified. Refer to the Managing Allegations Procedure from the LSCB to ensure the correct procedures are used with incidents of misuse (flowchart in Appendices).

Staff and Other Adults

It is the responsibility of all staff and other adults within the school to:

- Be familiar with the Behaviour, Anti-bullying and other relevant policies so that, in the event of misuse or an allegation, the correct procedures can be followed immediately. In the event that a procedure is unknown, they will refer to the Headteacher immediately, who must then follow the Managing Allegations Procedure, where appropriate.
- Check the filtering levels are appropriate for their children and young people and are set at the correct level. Report any concerns to the Online Safety Lead.
- Alert the Online Safety Lead of any new or arising issues and risks that may need to be included within policies and procedures.
- Ensure the tone of e-mails is appropriate, polite and in keeping with all other methods of communication
- Report inappropriate tones to the Head Teacher and/or Trustees.
- Ensure that children and young people are protected and supported in their use of technologies so that they know how to use them in a safe and responsible manner.
- Ensure pupils know what to do in the event of an incident.
- Be up-to-date with Online Safety knowledge that is appropriate for the age group and reinforce through the curriculum.
- Use electronic communications in an appropriate way that does not breach the Data Protection Act 1998.Remember confidentiality and not disclose information from the network, pass on security passwords or leave a station unattended when they or another user is logged in.
- Report accidental access to inappropriate materials to the Online Safety Lead. The Online Safety lead will then restrict access (if possible) or report this to the internet service provider so that inappropriate sites are added to the restricted list
- Use anti-virus software and check for viruses on their work laptop when transferring information from the internet on a regular basis, especially when not connected to the school's network.
- Ensure that all personal storage devices (i.e. memory sticks) which are utilised by staff members to hold sensitive information are encrypted or password protected in the event of loss or theft.

Children and Young People

Children and young people must be:

- Involved in the review of Acceptable Use Agreement through the school council or other appropriate group, in line with this policy being reviewed and updated.
- Responsible for following the Acceptable Use Agreement whilst within school as agreed at the beginning of each academic year or whenever a new child attends the school for the first time.
- Taught to use the internet in a safe and responsible manner through Computing, PSHE or other clubs and groups.
- Taught to tell an adult about any inappropriate materials or contact from someone they do not know straight away, without reprimand (age and activity dependent).

Appropriate and Inappropriate Use by Staff or Adults

All staff are required to sign to confirm that they have read, understood and will follow the Acceptable Use Agreement on an annual basis

In the Event of Inappropriate Use

If a member of staff is believed to misuse the internet or learning platform in an abusive or illegal manner, a report must be made to the Head Teacher immediately and then the Managing Allegations Procedure and the Safeguarding Policy must be followed to deal with any misconduct and all appropriate authorities contacted.

In the lesser event of misuse or accidental misuse refer to appendices for a list of actions relating to the scale of misuse.

By Children or Young People

The Acceptable Use Agreement is contained in the Appendices. The agreement is there for children to understand what is expected of their behaviour and attitude when using the internet. This will enable them to take responsibility for their own actions. For example, knowing what is polite to write in an e-mail to another

child, or understanding what action to take should there be the rare occurrence of sighting unsuitable material. This also includes the deliberate searching for inappropriate materials and the consequences for doing so.

An acceptable use agreement is sent out for new entrants to the school in their packs. Pupils new to the school will be asked to read and complete the acceptable use agreement at school within their first half term.

Further to this, it is hoped that parents/carers will add to future rule amendments or updates to ensure that they are appropriate to the technologies being used at that time and reflect any potential issues that parents/carers feel must be addressed, as appropriate.

The downloading of materials, for example, music files and photographs need to be appropriate and 'fit for purpose' based on research for work and be copyright free.

File-sharing via e-mail, weblogs or any other means online must be appropriate and be copyright free when using the learning platform in or beyond school.

In the Event of Inappropriate Use

Should a child or young person be found to misuse the online facilities whilst at school, the following consequences must occur

- Any child found to be misusing the internet by not following the Acceptable Use Agreement may have a letter sent home to parents/carers explaining the reason for suspending the child or young person's use for a particular lesson or activity.
- Further misuse of the agreement may result in not being allowed to access the internet for a period of time and another letter will be sent home to parents/carers.
- A letter may be sent to parents/carers outlining the breach in Safeguarding Policy where a child or young person is deemed to have misused technology against another child or adult.

In the event that a child or young person **accidentally** accesses inappropriate materials the child must report this to an adult immediately and take appropriate action to hide the screen, (dependent on age) so that an adult can take the appropriate action. The issue of a child or young person deliberately misusing online technologies must also be addressed by the establishment.

Children must be taught and encouraged to consider the implications for misusing the internet and posting inappropriate materials to websites, for example, as this may have legal implications.

The Curriculum and Tools for Learning

Internet Use

Schools will teach children and young people how to use the Internet safely and responsibly. They must also be taught, through Computing and/or PSHE lessons, how to research information, explore concepts and communicate effectively in order to further learning. The following concepts, skills and competencies will have been taught by the time they leave Year 6

- Internet literacy.
- Making good judgements about websites and e-mails received.
- Knowledge of risks such as viruses and opening mail from a stranger.
- Access to resources that outline how to be safe and responsible when using any online technologies.
- Knowledge of copyright and plagiarism issues.
- File sharing and downloading illegal content.
- Uploading information – know what is safe to upload and not upload personal information.
- Where to go for advice and how to report abuse.

Online Safety lessons and resources can also be found at www.thinkuknow.co.uk for KS1 and KS2.

These skills and competencies are taught within the curriculum so that children and young people have the security to explore how online technologies can be used effectively, but in a safe and responsible manner.

Children and young people must know how to deal with any incidents with confidence, as we adopt the 'never blame the child for accidentally accessing inappropriate materials' culture, in the event that they have **accidentally** accessed something.

School Website

The uploading of images to the school website must be subject to the same acceptable agreement as uploading to any personal online space. Permission must be sought from the parent/carer prior to the uploading of any images unless permission has been given at the start of the year by completion of the consent letter by a parent. Schools must consider which information is relevant to share with the general public on a website and use secure areas for information pertaining to specific audiences.

External Websites

In the event that a member of staff finds themselves or another adult on an external website, as a victim, staff are encouraged to report incidents to the Head Teacher and unions, using the reporting procedures for monitoring.

Mobile Phones and Other Emerging Technologies

Pupils are not permitted to bring mobile devices to school unless they are required to contact parents at the end of the school day. These devices must be stored securely in school office during the day and collected at the end of school.

Mobile phone and other personal technological devices are not permitted to be used in the school or on school premises by pupils during school hours without the permission of either the Headteacher or most senior member of staff.

Staff may bring mobile devices to school and use these before and after school, during their break time (unless they are on break duty) and during their PPA time but must not use mobile phones during lessons, this includes sending and reading text messages unless this has been authorised by the Headteacher or most senior teacher on site.

Personal phones and other camera devices must not be used for taking pictures during school time unless this has been authorised by the Headteacher or most senior teacher on site.

Video and Photographs

The term 'image' refers to the taking of video footage or photographs via any camera or other technology, e.g. a mobile phone.

The office keeps a log of parental permissions which is updated at least annually - it is important that this list is checked before uploading of images takes place. Permission from the Headteacher for uploading of images to the website must be sought prior to doing so.

Any photographs or video clips uploaded must not have a file name of a child, especially where these may be uploaded to a school website. Photographs must not be named with the child's name or contain any text which allows the child's name to be identified.

Group photographs are preferable to individual children and young people and must not be of any compromising positions or in inappropriate clothing, e.g. swimwear. All photos of pupils taken will be stored on the school's network which has only staff access. These photos and videos will be deleted after a year or when the pupil leaves the school, whichever is the latter.

It is current practice by external media such as local and national newspapers to include the full name of children and young people in their publications. Photographs of children/young people must only be used after permission has been given by a parent/carer.

Video-Conferencing and Webcams

All use of webcams must be supervised by a teacher as part of a class session.

Managing Social Networking

Social networking is used by the school for marketing purposes. No other social networking sites are to be accessed in school by staff, pupils or others without the permission of the Headteacher.

Social Networking Advice for Staff

Social networking outside of work hours, on non school-issue equipment, is the personal choice of all school staff. Owing to the public nature of such websites, it is advisable for staff to consider the possible implications of participation. The following advice must be considered if involved in social networking:

- Personal details are never shared with pupils such as private email address, telephone number or home address. It is recommended that staff ensure that all possible privacy settings are activated to prevent students from making contact on personal profiles. The simplest and most effective way to do this is to remove details from search results and turn off public visibility.
- Staff must not engage in personal online contact with pupils until written permission has been received from the headteacher
- Staff must ensure that full privacy settings are in place to prevent students from accessing photo albums or personal information.
- Staff are advised against accepting invites from colleagues until they have checked with them in person that the invite is genuine (avoiding fake profiles set up by students).

Safeguarding Measures – Filtering

Staff, children and young people are required to use the personalised learning space and all tools within it, in an acceptable way.

The school utilises the Fortigate content filtering solution. The filtering is cloud based and protects any device linked to the schools' network without the need for additional configuration. It uses filter categories that are being maintained by identification by both Web and IP Reputation and Web Classification services. The sites identified in these filter categories are then blocked to prevent access to websites containing, for example, offensive materials (such as pornographic or violent imagery), distracting or time-wasting materials (such as social networking and non-educational games) and downloads of certain types of files (such as program or music files). The filter categories are constantly evolving and updates are automatically applied whenever a URL is requested. If a website needs blocking because of inappropriate content, then please email the following address Sandra.Mackay@rad-group.co.uk. They will block and then send you a confirmation email.

Monitoring
The Governor for Safeguarding should regularly review the effectiveness of school filters and monitoring systems. They should ensure that the leadership team and relevant staff are:

• aware of and understand the systems in place
• manage them effectively
• know how to escalate concerns when identified.

The Online Safety Lead and/or a senior member of staff must be monitoring the use of online technologies by children and young people and staff, on a regular basis.

Teachers must monitor the use of the learning platform and Internet during lessons and also monitor the use of e-mails from school and at home, on a regular basis.

Parents – Roles

Each child or young person will receive a copy of the Acceptable Use Agreement on first-time entry to the school which needs to be read with the parent/carer, signed and returned to school, confirming both an understanding and acceptance of the agreement.

It is expected that parents/carers will explain and discuss the agreement with their child, where appropriate, so that they are clearly understood and accepted.

The schools will keep a record of the signed forms.

Support

Schools may choose to follow or adapt this guidance:

As part of the approach to developing Online Safety awareness with children and young people, the school may offer parents the opportunity to find out more about how they can support the school in keeping their child safe and find out what they can do to continue to keep them safe whilst using online technologies beyond school. The school may want to promote a positive attitude to using the World Wide Web and therefore want parents to support their child's learning and understanding of how to use online technologies safely and responsibly. The school will do this by sending out regular up to date information to parents regarding internet safety.

This will provide parents with information on how the school protects children and young people whilst using the learning platform facilities, such as the Internet. It will also explore how the school is teaching children and young people to be safe and responsible Internet users and how this can be extended to use beyond the school environment.

Links to Other Policies - Behaviour and Anti-Bullying Policies

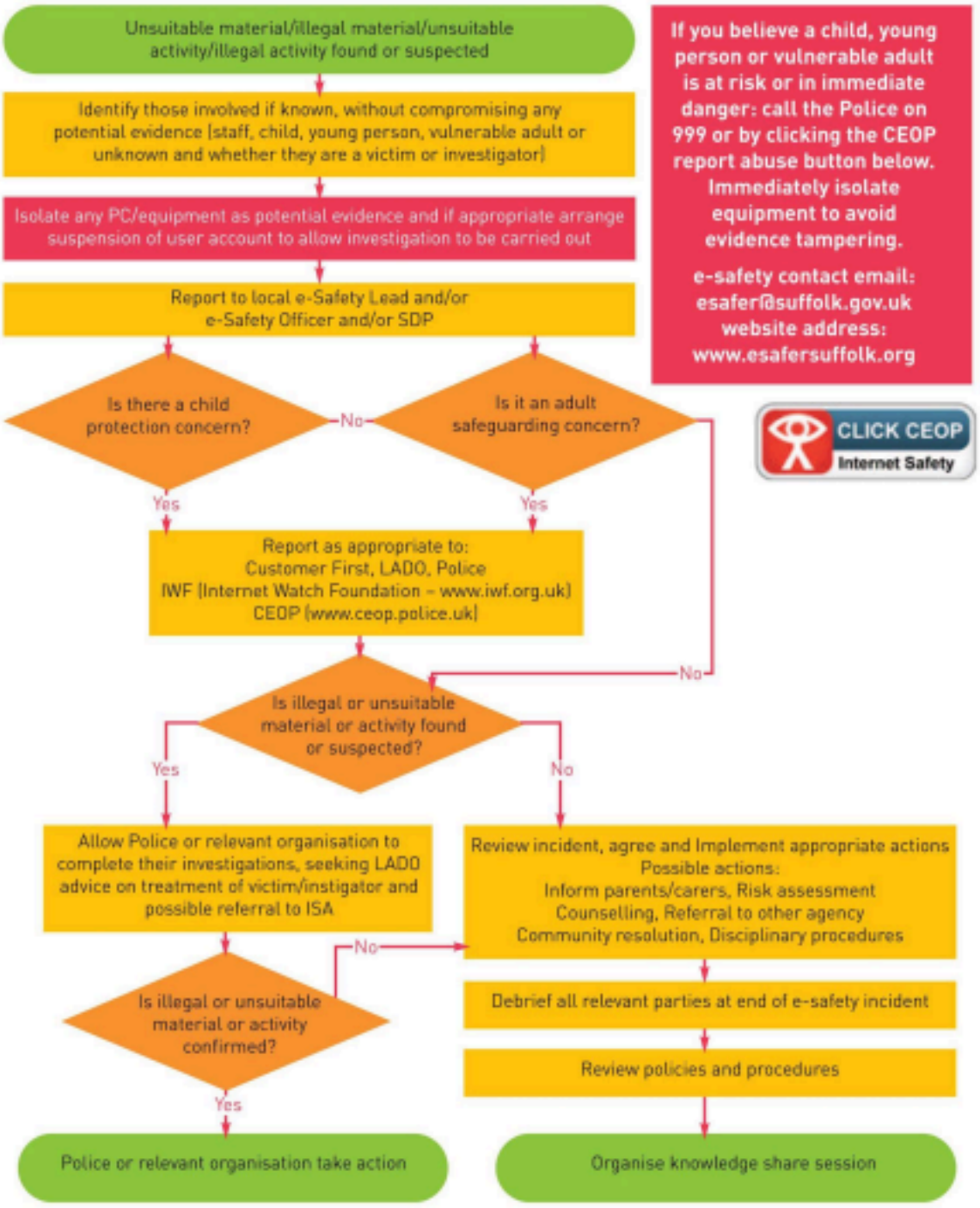
This policy must be read in conjunction with the Safeguarding Policy, Behaviour Policy and Anti-bullying Policy.

Curriculum Development

The teaching and learning of Online Safety must be embedded within the school/education establishment curriculum to ensure that the key safety messages about engaging with people are the same whether children and young people are on or off line. This may form part of the PHSE module but is not exclusive to this area of curriculum and opportunities to embed Online Safety throughout the curriculum should be sought.

Appendix 1: Online Safety Flow Chart

e-Safety Incident Flowchart



If you believe a child, young person or vulnerable adult is at risk or in immediate danger: call the Police on 999 or by clicking the CEOP report abuse button below. Immediately isolate equipment to avoid evidence tampering.

e-safety contact email: esafer@suffolk.gov.uk
website address: www.esafersuffolk.org

CLICK CEOP
Internet Safety

Appendix 2.

Acceptable Use Agreement for Trustees, SGC members and Volunteers.

This agreement applies to all online use and to anything that may be downloaded or printed.

All adults within the school must be aware of their safeguarding responsibilities when using any online technologies, such as the internet, E-mail or social networking sites. They are asked to sign this Acceptable Use Agreement so that they provide an example to children and young people for the safe and responsible use of online technologies. This will educate, inform and protect adults so that they feel safeguarded from any potential allegations or inadvertent misuse themselves.

1. I know that I must only use the school equipment in an appropriate manner and for professional uses.
2. I know that images must not be inappropriate or reveal any personal information of children and young people if uploading to the internet.
3. I have read the Online Safety Incident flowchart so that I can deal with any problems that may arise, effectively.
4. I will report accidental misuse.
5. I will report any incidents of concern for a child or young person's safety to the Head
6. I know my Designated Safeguarding Lead
7. I know the Online Safety Lead is Andrew Berry.
8. I know that I am putting myself at risk of misinterpretation and allegation if I contact children and young people via personal technologies, including my personal e-mail (inside and outside of school). 9. I know that I must not use the school system for personal use unless this has been agreed by the Head of School or Online Safety Lead.
10. I know that I must complete virus checks on my memory stick or other devices so that I do not inadvertently transfer viruses, when using these on school devices
11. I will follow Data Protection legislation
12. Any confidential information that I store on a device will be password protected. 13. I will ensure that I follow the Data Protection Act 1998 and have checked I know what this involves. 14. I will adhere to copyright and intellectual property rights.
15. I will only install hardware and software I have been given permission for by the Principal. 16. I accept that the use of any technology designed to avoid or bypass the school filtering system is forbidden. I understand that intentional violation of this rule may result in disciplinary procedures being initiated.
17. I understand the Online Safety issues and procedures that I must follow.

I have read, understood and agree with these Agreement as I know that by following them I have a better understanding of Online Safety and my responsibilities to safeguard children and young people when using online technologies.

Signed…… Date…….

Name (printed)…….

Appendix 3

Acceptable Use Policy for Pupils

My Online Safety Agreement

This is my agreement for using the internet safely and responsibly and covers.

● I will use the internet to help me learn.
● I will learn how to use the internet safely and responsibly. ● I will only send email messages that are polite and friendly. ● I will only email, chat to, send images to or video-conference people that a trusted adult has approved.
● I agree never to give out passwords or personal information like my full name, address or phone numbers.
● I agree never to post photographs or video clips without permission
● If I need help I will ask a trusted adult
● I know that I can go to www.thinkuknow.co.uk for help if I cannot talk to a trusted adult.
● If I see anything on the internet that makes me feel uncomfortable, I will report this to a trusted adult immediately and not share it with anyone else.
● If I receive a message sent by someone I don't know, I will report this to a trusted adult
● I will not bring or use any personal devices at school without permission from the Head
● I know I must follow these guidelines as part of the agreement with my parent/carer.
● I agree to look after myself and others by using my internet in a safe and responsible way.
● I agree not to put any information online that could upset others or the school

Signed..... Dated.....

Name.....(Printed)

Appendix 4

Tilian Acceptable Use Agreement for Staff

This agreement applies to all online use and to anything that may be downloaded or printed.

All adults within the school must be aware of their safeguarding responsibilities when using any online technologies, such as the internet, E-mail or social networking sites. They are asked to sign this Acceptable Use Agreement so that they provide an example to children and young people for the safe and responsible use of online technologies. This will educate, inform and protect adults so that they feel safeguarded from any potential allegations or inadvertent misuse themselves.

1. I know that I must only use the school equipment in an appropriate manner and for professional uses. 2. I understand that I need to give permission to children and young people before they can upload images (video or photographs) to the internet or send them via E-mail.
3. I know that images must not be inappropriate or reveal any personal information of children and young people if uploading to the internet.
4. I have read the Online Safety Incident Flowchart (Appendix 1 of Online Safety Policy) so that I can deal with any problems that may arise, effectively.
5. I will report accidental misuse.
6. I will report any incidents of concern for a child or young person's safety to the Principal, in accordance with procedures listed in the Acceptable Use Policy.
7. I know my Designated Safeguarding Lead and Online Safety Lead is Andrew Berry.
8. I know that I am putting myself at risk of misinterpretation and allegation if I contact children and young people via personal technologies, including my personal e-mail.
9. I know I must use the school e-mail address and only to a child's school e-mail address upon agreed use within the school.
10. I know that I must not use the school system for personal use unless this has been agreed by the Head of School and/or Online Safety Lead.
11. I know that I must complete virus checks on my memory stick or other devices so that I do not inadvertently transfer viruses, especially where I have downloaded resources.
12. I will password protect memory sticks and confidential information
13. I will ensure that I follow the Data Protection Act 1998 and have checked I know what this involves. 14. I will ensure that I keep my password secure and not disclose any security information unless to appropriate personnel. If I feel someone inappropriate requests my password I will check with the Online Safety Lead prior to sharing this information.
15. I will adhere to copyright and intellectual property rights.
16. I will only install hardware and software I have been given permission for.
17. I accept that the use of any technology designed to avoid or bypass the school filtering system is forbidden. I understand that intentional violation of this rule may result in disciplinary procedures being initiated. 18. I understand the Online Safety issues and procedures that I must follow.

I have read, understood and agree with these Agreement as I know that by following them I have a better understanding of Online Safety and my responsibilities to safeguard children and young people when using online technologies.

Signed…….. Date…….

Name (printed)……