Bures CEVC Primary School

Online Safety Policy

Bures CEVC Primary School Governing Body have agreed and adopted this policy as part of their on-going commitment in ensuring excellence and best practice of current legislation is employed throughout the school.

Introduction

As part of Keeping Children Safe in Education (2016) legislation set out by the Government, the Education Act 2002 and the Children's Act 2004, it is the duty of a school to ensure that children and young people are protected from potential harm both within and beyond the school. Therefore, the involvement of all - children, young people and parent/carers is vital in order to successfully safeguard children while they use online technologies.

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 School

Governors and the Headteacher

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

- The Headteacher has designated an Online Safety Lead to implement agreed policies, procedures, staff training, curriculum requirements and take responsibility

for ensuring Online Safety is addressed in order to establish a safe ICT learning environment. All staff and students are aware of this role within the school.

- The Headteacher will report breaches to this policy, with support from the Online Safety Lead, as outlined in Appendix 4.
- The Headteacher, will ensure that there is a standard disclaimer on all e-mails stating that the views expressed are not necessarily those of the school.
- Time and resources should be provided for the Online Safety Lead and staff to be trained and update policies, where appropriate.
- The Headteacher is responsible for promoting Online Safety across the curriculum and has an awareness of how this is being developed, linked with the School Development and Improvement Plan.
- The Headteacher should inform the Governors at the Curriculum, Performance and Personnel Committee meetings about the progress of or any updates to the Online Safety curriculum (via PSHE or ICT) and ensure Governors know how this relates to safeguarding. At the Full Governing Body meetings, all Governors are to be updated of Online Safety developments from the committee meetings.
- The Governors **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 Governors to ensure that all safeguarding guidance and practices are embedded.
- Governors receive an update to the Online Safety incidents that have taken place in the School through the Safeguarding Report which is uploaded to GovernorHub, as an appendix to the Headteacher's Report.
- An Online Safety Governor (can be the Computing or Safeguarding Governor) challenges the school about the appropriate strategies which define the roles, responsibilities for the management, implementation and safety for using ICT, including:

  Challenging the school/education setting or other establishment about having:

  - Firewalls.
  - Anti-virus and anti-spyware software.
  - Filters.
  - Using an accredited ISP (Internet Service Provider).
  - Awareness of wireless technology issues.
  - A clear policy on using personal devices (included in this policy and the Behaviour Policy).
- 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 agreed protocols) or involving parents/carers.

Local Online Safety Lead

In our School:

- Ms Emma Holtom is the Online Safety Lead;
- Mrs Karen White is the Online Safety Governor.

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

- 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 this policy is reviewed annually, with up-to-date information and that training is available for all staff to teach Online Safety and for parents to feel informed and know where to go for advice;
- Ensure that the technician makes certain that all filtering is set to the correct level for staff, children and young people (EYFS/KS1/KS2 Adult), in the initial set up of a network, stand-alone PC, staff/children laptops and the learning platform*;*
- Ensure that all adults are aware of the filtering levels and why they are there to protect children and young people.
- Report issues and updates the Headteacher on a regular basis, as outlined in Appendix 4. The Online Safety Lead should assist staff in completing Online Safety Incident Referral Forms (see Appendix 5) if a safeguarding incident takes place where technology is involved. This must be passed to the Designated Safeguarding Lead, as outlined in the Safeguarding Policy. Information regarding Online Safety Incidents should be recorded in the Headteacher / Safeguarding Governor's Safeguarding Report to Governors.
- Liaise with the PSHE lead and DSL so that policies and procedures are up-to-date to take account of any emerging issues with technologies.
- Update staff training (all staff) according to new and emerging technologies so that the correct Online Safety information can be taught or adhered to.
- Monitoring of Internet and online technology use, as recorded and reportable by the technician.
- Keep a log of incidents (see Appendix 6) for analysis to help inform future development and safeguarding, where risks can be identified. Refer to the Managing Allegations Procedure from the SSCB to ensure the correct procedures are used with incidents of misuse.
- Ensure, alongside the technician, that there is appropriate and up-to-date anti-virus software and anti-spyware on the network, stand-alone PCs and teacher/child laptops and that this is reviewed and updated on a regular basis.
- Ensure that staff can check for viruses on laptops, stand-alone PCs and (encrypted) memory sticks or other transferable data files to minimise issues of virus transfer.
- Ensure that inappropriate and / or unsolicited e-mails to any member of staff from other sources is reported immediately to the Headteacher. Refer to the Managing Allegations Procedure, SSCB, for dealing with any issues arising from indecent or pornographic/child abuse images sent/received.

- Arrange the annual parent / carer Online Safety Information event.

Staff or Adults

It is the responsibility of all adults within the school to:

- Ensure that they know who the Senior Designated Person for Safeguarding is within school, so that any misuse or incidents can be reported which involve a child. This includes where the use of technology has been utilised to do this;
- Where an allegation is made against a member of staff it should be reported immediately to the Headteacher/Senior Designated Person;

  In the event of an allegation made against the Headteacher, the Chair of Governors must be informed immediately;
- Be familiar with the Safeguarding Policy, Behaviour Management Policy 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/Senior Designated Person immediately, who should then follow the Safeguarding or 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 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. Children and young people should 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.
- Sign an Acceptable Use Statement to show that they agree with and accept the agreement for staff using non-personal equipment, within and beyond the school as outlined in Appendix 2. In addition, all staff and Governors are expected to sign the Staff, Governors and Visitors Code of Conduct.
- 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.
- To ensure that the School Business Manager follows the correct procedures for any data required to be taken from the school.
- Report accidental access to inappropriate materials to the Online Safety Lead in order that inappropriate sites are added to the restricted list or control this with the Local Control options via the broadband connection.
- Use anti-virus software and check for viruses on their work laptop, memory stick or a CD ROM 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.
- Report incidents to the Online Safety Lead and Headteacher of personally directed "bullying" or other inappropriate behaviour via the Internet or other technologies using the SCC accident/incident reporting procedure in the same way as for other non-physical assaults. The Online Safety Lead should assist staff in completing Online Safety Incident Referral Forms (see Appendix 5) if a safeguarding incident takes place where technology is involved. This must be passed to the Designated Safeguarding Lead, as outlined in the Safeguarding Policy.

Children and Young People

Children and young people should be:

- Involved in the review of the Pupil Online Safety Agreement through the School Council, in line with this policy being reviewed and updated.
- Responsible for following the Pupil Online Safety 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

Staff members have access to the network so that they can obtain age appropriate resources for their classes and create folders for saving and managing resources in the appropriate drives.

They have a password to access a filtered internet service and know that this should not be disclosed to anyone or leave a computer or other device unattended whilst they are logged in.

All staff receive a copy of the Acceptable Use Policy (see Appendix 2) annually and should return a signed copy of the agreement to the School which should be kept.

In the Event of Inappropriate Use

All staff should use technology appropriately as outlined in Appendix 4.

If a member of staff is believed to have misused the internet in an abusive or illegal manner, a report must be made to the Headteacher/Senior Designated Person immediately and then the Managing Allegations Procedure and the Safeguarding Policy must be followed to deal with any misconduct and all appropriate authorities contacted. The Flow Chart as outlined in Appendix 1 should be followed.

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

Appropriate and Inappropriate Use By Children or Young People

The School has adopted a Pupil Online Safety Agreement that should be signed by all children and their parents annually each September or whenever a new pupil joins the School (see Appendix 3). This details how children and young people are expected to use the internet and other technologies within school/education setting or other establishment, including downloading or printing of any materials. The agreements are there for children and young people 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.

The School encourages parents/carers to support the agreement with their child or young person. This is shown by a joint signing of the Pupil Online Safety Agreement so that it is clear to the School that the agreement is accepted by the child with the support of the parent/carer. This is also intended to provide support and information to parents/carers when children and young people may be using the Internet outside school.

Further to this, through the annual consultation process, 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 should 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 should be appropriate and be copyright free when using the learning platform in or beyond school/education setting or other establishment.

In the Event of Inappropriate Use

All pupils should keep to the agreed ICT usage as outlined in Appendix 4.

Should a child or young person be found to misuse the online facilities whilst at school, and in breach of the Pupil Online Safety Agreement, that child may have their online access temporarily removed and 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 the child not being allowed to access the internet for a period of time and another letter will be sent home to parents/carers.
A further letter may be sent to parents/carers outlining the breach of the 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 should report this to an adult immediately and take appropriate action to hide the screen or close the window, e.g. use 'Hector Protector', for example, (dependent on age) so that an adult can take the appropriate action. Where a child or young person feels unable to disclose abuse, sexual requests or other misuses against them to an adult, they can use the Report Abuse button (www.thinkuknow.co.uk) to make a report and seek further advice;

from the NSPCC. The issue of a child or young person deliberately misusing online technologies should also be addressed by the school.

Children should 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
Our School teaches children and young people how to use the Internet safely and responsibly through our Cornerstones curriculum. They are also taught, through computing lessons, how to research information, explore concepts and communicate effectively in order to further learning. The following concepts, skills and competencies should 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.

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 should 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.

Personal safety – ensuring information uploaded to websites and e-mailed to other people does not include any personal information such as:

- Full name (first name is acceptable, without a photograph).
- Address.
- Telephone number.
- E-mail address.
- School/education setting or other establishment.
- Clubs attended and where.
- Age or DOB.
- Names of parents.
- Routes to and from school/education setting or other establishment.
- Identifying information, e.g. I am number 8 in the school/education setting or other establishment Football Team.

Photographs should only be uploaded on the approval of a member of staff or parent/carer and should only contain something that would also be acceptable in 'real life'.
Parents/carers should monitor the content of photographs uploaded. Images of children and young people should be stored according to the School's digital imaging and data

protection policies. Please see the school's Digital Imaging and Recording Policy and Data Protection Policy.

Pupils with Additional Learning Needs

The School strives to provide access to a broad and balanced curriculum for all learners and recognises the importance of tailoring activities to suit the educational needs of each pupil. This is achieved through our Cornerstones curriculum. Where a student has specific learning requirements, or poor social understanding, careful consideration is given to the planning and delivery of Online Safety awareness sessions and internet access.

School Website

The uploading of images to the school website is subject to the same acceptable agreement as uploading to any personal online space. Permission is sought from the parent/carer prior to the uploading of any images, through the signed parent consent form obtained at the beginning of each academic year or whenever a child joins the School.

External Websites / Social Media

In the event that a member of staff finds themselves or another adult on an external website or social media, such as 'Rate My Teacher' or Facebook, as a victim, schools are encouraged by Suffolk Local Authority to report incidents to the Headteacher and unions, using the reporting procedures for monitoring.

E-mail Use

The School has e-mail addresses for children and young people to use, as a class and/or as individuals as part of their entitlement to being able to understand different ways of communicating and using ICT to share and present information in different forms.

Individual email accounts can be traced if there is an incident of misuse whereas class email accounts cannot, especially for older users.

Staff, children and young people should use their school issued email addresses for any communication between home and school only. A breach of this may be considered a misuse.

Parents/carers are actively encouraged to be involved with the monitoring of emails sent, although the best approach with children and young people is to communicate about who they may be talking to and assess risks together.

Teachers are expected to monitor their class use of emails where there are communications between home and school, as necessary. As the School has a network manager, there is an expectation that monitoring software is used to flag up inappropriate terms and that a senior member of the team has an overview of potential issues on a regular basis – refer to the Monitoring section for further information.

Mobile Phones and Other Emerging Technologies

School should carefully consider how the use of mobile technologies can be used as a teaching and learning tool within the curriculum with the following areas of concern to be taken into consideration:

- Inappropriate or bullying text messages.
- Images or video taken of adults or peers without permission being sought.
- 'Happy slapping' – the videoing of violent or abusive acts towards a child, young person or adult which is often distributed.
- Sexting - the sending of suggestive or sexually explicit personal images via mobile phones.
- Wireless Internet access, which can bypass school filtering and allow access to inappropriate or potentially harmful material or communications.

The School does not as everyday practice encourage the use of mobile phones or tablet devices by children during school hours. This is due to the increased incidents of bullying and misuse have been reported where students are allowed to use them in school. In settings where clear agreement on this issue are agreed to and followed, the level of misuse is reduced. Where inappropriate usage of said technologies does occur a virtual paper trail may be traceable, even if the message received is sent anonymously.

Personal Mobile Devices

Staff and visitors should be allowed to bring in personal mobile phones or devices for their own use, but **must not use personal numbers to contact children and young people under any circumstances. They must not take photographs of children on these devices.**

- Staff and visitors must ensure that there is no inappropriate or illegal content stored on the device and should be aware that using features, such as video or sound recording, may be subject to the same procedures as taking images from digital or video cameras.
- Staff and visitors should be aware that games consoles such as the Sony Play Station, Microsoft Xbox, Nintendo Wii and DSi and other such systems have Internet access which may not include filtering. Before use within school, authorisation should be sought from the Headteacher and the activity supervised by a member of staff at all times.
- The school is not responsible for any theft, loss or damage of any personal mobile device.

School Issued Mobile Devices

The management of the use of these devices should be similar to those stated above, but with the following additions:

- Where the establishment has provided a mobile device to a member of staff, such as a laptop, tablet or mobile phone, only this equipment should be used to conduct school business outside of the school environment.

It should also be policy to ensure that children and young people understand the use of a public domain and the consequences of misuse. Relevant curriculum links should be made to highlight the legal implications and the involvement of law enforcement. Other technologies which school use with children and young people include:

- iPads;
- Photocopiers;
- Telephones;
- Cameras;
- GPS watches.

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.

When in school/ setting there is access to:
- Digital cameras;
- iPads;
- Laptops;
- Webcams;
- Visualisers;
- Interactive televisions.

It is also highly recommended that permission is sought prior to any uploading of images to check for inappropriate content.

The sharing of photographs via blogs, forums or any other means online should only occur after permission has been given by a parent/carer or member of staff (as appropriate).

Photographs/images used to identify children and young people in a forum or using Instant Messaging within the learning platform should be representative of the child rather than of the child e.g. an avatar.

Any photographs or video clips uploaded should not have a file name of a child, especially where these may be uploaded to a school website. Photographs should only ever include the child's first name although safeguarding guidance states either a child's name or a photograph but not both.

Group photographs are preferable to individual children and young people and should not be of any compromising positions or in inappropriate clothing. The School has decided how photographs will be used, where they will be stored on the school network and that they will be deleted once the child leaves school.

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 should only be used after permission has been given by a parent/carer.

Please also see the School's Digital Imaging and Recording Policy.

Video-Conferencing and Webcams

Flashmeeting is the main video conferencing service provided by E2BN which allows staff to preset a secure 'conference room' which remains under their control throughout the

session. The use of webcams to video-conference will be via E2BN which is a filtered service. Publicly accessible webcams are not used in school.

Taking images via a webcam should follow the same procedures as taking images with a digital or video camera.

Permission should be sought from parents and carers if their child is engaged in video conferencing with individuals or groups outside of the school. This process should always be supervised by a member of staff and a record of dates, times and participants held by the school.

Children need to tell an adult immediately of any inappropriate use by another child or adult (this is part of the Pupil Online Safety Agreement).

Where children, young people (or adults) may be using a webcam in a family area at home, they should have open communications with parents/carers about their use and adhere to the Pupil Online Safety Agreement.

Managing Social Networking and Other Web Technologies

Social networking sites have emerged in recent years as a leading method of communication proving increasingly popular amongst both adults and young people alike. The service offers users both a public and private space through which they can engage with other online users. With responsible use, this technology can assist with the development of key social skills whilst also providing users with access to a range of easily accessible, free facilities. However, as with any technology that opens a gateway to online communication with young people, there are a number of risks associated which must be addressed.

With this in mind, both staff and pupils are encouraged to think carefully about the information which they provide on such websites and the way in which it can be manipulated when published (examples of which include Facebook, Snapchat and Instagram). The School does not allow children to use open-public Social Media sites in School and discourages the use of Social Media sites outside of School, as the sign-up age for most sites is 14 years of age.

In response to this issue the following measures should be put in place:

- Where a learning-based, primary-school based social media site is used, strict access and control is maintained through existing filtering systems. Students are advised against giving out personal details or information, which could identify them or their location (e.g. mobile phone number, home address, school name, groups or clubs attended, email address or full names of friends).
- Students are discouraged from posting personal photos on social networking sites without considering how publicly accessible the information is and the potential for misuse. Advice is also given regarding background images in photos, which could reveal personal details (e.g. house number, street name, school uniform).
- Pupils are advised on social networking security and recommendations made for privacy settings to be activated to 'Friends only' for all applications to restrict unsolicited access. The importance of passwords and blocking of unwanted communications is also highlighted.
- The school is aware that social networking can be a vehicle for cyber bullying. Pupils are encouraged to report (and save and take a screen shot of) any incidents of

bullying to the School allowing for the procedures, as set out in the School's Behaviour Management Policy, to be followed.

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. All staff sign the Staff and Visitors' Code of Conduct. The following advice should 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 should not engage in personal online contact with students outside of Headteacher authorised systems (e.g. school email account for homework purposes).
- Staff should 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

The E2BN broadband connectivity has a filter system which is set at an age appropriate level so that inappropriate content is filtered and tools are appropriate to the age of the child. **All** filtering is set to 'No Access' within any setting and then controlled via:

- Portal Control (controls filtering at local site level) which controls individual access to the Internet. This also links to the E2BN criteria 'Schedule 11' of Level Four site filtering to qualify for access to the broadband services.
- Local Control – controls access to websites and provides the option to add to a 'restricted list'.

The Headteacher should sign a disclaimer stating agreement to the filtering levels being maintained as part of the connectivity to broadband requirements from E2BN-pl. In the event that the site level is not set to 'No Access', the Headteacher and Governors should write a letter to the LA to explain how they intend to safeguard their children and young people. E.g. Use an appropriate accredited service such as Netsweeper or school guardian so that the minimum of Beta Level Four is met.

The levels listed below are in relation to age-appropriate categories:

Level One	E2BN standard basic minimum adult policy.
Level Two	E2BN standard senior pupils' policy; Key Stage 2
Level Three	E2BN standard younger pupils' policy; Key Stage 1
Level Four	E2BN standard young pupil's policy; EYFS

No search, no politics and religion.

This complies with the agreed connectivity legalities with Synetrix and E2BN and also ensures our younger audiences are not exposed to unnecessary risks e.g. a blanket Level Two for Primary school users, is inappropriate.

Anti-virus and anti-spyware software is used on all network and stand-alone PCs or laptops and is updated on a regular basis.

A firewall ensures information about children and young people and the school/education or other establishment cannot be accessed by unauthorised users.

The 'skin' of the online personal space is age appropriate and only tools appropriate to the age of the child are available.

An RSS (Really Simple Syndication) feed provides a direct link to commonly used websites so that children and young people do not need to leave their personal space for updates.

Children should use a search engine that is age appropriate such as AskJeeveskids, Yahooligans or Googlekidsearch.

Links or feeds to Online Safety websites are provided. Hector Protector should be used as a screen cover so that anything accidentally accessed can be covered whilst an adult is informed. Encryption codes on wireless systems are used in the School to prevent hacking.

For older children and young people, the Report Abuse button is available should there be a concern of inappropriate or malicious contact made by someone unknown. This provides a safe place for children and young people to report an incident if they feel they cannot talk to a known adult.

CEOP (Child Exploitation and Online Protection Centre) awareness training is given to all Key Stage 1 and 2 pupils as appropriate and recommended as part of the computing curriculum, for raising awareness on staying safe and being responsible. A link to the www.thinkukknow.co.uk website is part of the skin layout for further advice and information on children or young people's personal online spaces.

Tools for Bypassing Filtering

Web proxies are probably the most popular and successful ways for students to bypass Internet filters today, identifying a cause for concern amongst schools, where children and young people can access the Internet. Web proxies also provide an anonymous route through filtering safeguards in existence on networked facilities, allowing users to navigate through potentially harmful or inappropriate content.

A web proxy is capable of hiding the IP address of the user and opening unrestricted and, in some cases, unidentifiable channels through which material can be viewed. The most common use of this tool amongst students is to access social networking features, gaming websites or information of an adult nature- all of which is blocked through the school's filtering system.

The technician monitors this situation and will make any amendment to practice where it is viewed that an improvement can be made.

Students and staff are forbidden to use any technology designed to circumvent, avoid or bypass any school security controls (including internet filters, antivirus solutions or firewalls) as stated in the Pupil Online Safety Agreement.

Violation of this rule will result in disciplinary or in some circumstances legal action.

As a School, we are aware that block banning of a pupil's ICT or internet access can be severely disruptive to learning across the curriculum and can also affect lesson planning and is therefore only applied in the most serious breaches.

Monitoring

The Online Safety Lead with support of the technician, monitors the use of online technologies by children and young people and staff, on a regular basis.
The Online Safety Lead with support of the technician, monitors the use of the internet on a regular basis, with alerts sent in real-time to highlight any potential misuse or risk.

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

IT Suite

The computers in the School's IT Suite are protected in line with the school network.
Where software is used that requires a child login, this is password protected so that the child is only able to access themselves as a user. Children and young people are taught not to share passwords.

Parents – Roles

Each child or young person receives a copy of the Pupil Online Safety Agreement on an annual basis or at 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 should be expected that parents/carers will explain and discuss the agreement with their child, where appropriate, so that they are clearly understood and accepted.
The School keeps a record of the signed forms in the School Office.

Support

As part of the approach to developing Online Safety awareness with children and young people, the School offers 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 promotes 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. We as a School do this by holding an Online Safety Parent/Carer Information event once per annum.

Part of this event will provide parents with information on how the school protects children and young people whilst using the Internet and E-mail. It is also an opportunity to 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.

Resources

The School:

- Can use the Childnet International 'KnowITAll for Parents' CD/online materials (http://www.childnet-int.org.uk/kia/parents/cd/) to deliver key messages and raise awareness for parents/carers and the community.
- Ensure that skills around internet use are offered for parents/carers so they know how to use the tools their children and young people are using.
- Endeavour to provide access to the internet for parents/carers so that appropriate advice and information can be accessed where there may be no internet at home, subject to arrangement.

Links to Other Policies – Behaviour Management Policy

Please refer to the Behaviour Management Policy for the procedures in dealing with any potential bullying incidents via any online communication, such as mobile phones, e-mail or blogs.

All behaviours are seen and dealt with in exactly the same way, whether on or off-line and this is a key message which sits within our computing curriculum. Staff do not treat online behaviours differently to off-line behaviours and should have exactly the same expectations for appropriate behaviour. This is a key message which is reflected within the Safeguarding Policy and the Behaviour Management Policy, as it is only the tools and technologies that change, not the behaviour of children, young people and adults.

Managing Allegations against Adults Who Work With Children and Young People

Please refer to the Managing Allegation Procedure, in order to deal with any incidents that occur as a result of using personal mobile or e-mail technologies. The procedures detail how to deal with allegation of misuse or misconduct being made by any member of staff or child about a member of staff.

Allegations made against a member of staff should be reported to the Designated Safeguarding Lead (DSL) within the school immediately. In the event of an allegation being made against a Headteacher, the Chair of Governors should be notified immediately.

Local Authority Designated Officer (LADO) - Managing Allegations:

The Local Authority has designated Officers who are involved in the management and oversight of individual cases where there are allegations against an adult in a position of trust. They provide advice and guidance to all of the above agencies and services, and monitor the progress of the case to ensure all matters are dealt with as quickly as possible, consistent with a thorough and fair process. In addition to this they liaise with the police and other agencies.

Disciplinary Procedure for All School Based Staff

In the event that a member of staff may be seen to be in breach of behaviour and good conduct through misuse of online technologies, this policy outlines the correct procedures for ensuring staff achieve satisfactory standards of behaviour and comply with the rules of the Governing Body.

Curriculum Development
The teaching and learning of Online Safety is embedded within the school 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. Opportunities to embed Online Safety throughout the curriculum are sought by class teachers.

Health and Safety

Refer to the Health and Safety Policy and procedures of the school and the County Council for information on related topics, particularly Display Screen Equipment, Home working and Accident/Incident reporting procedures. Wireless technologies are not considered to be a hazard following advice from the Health Protection Agency to the Government.

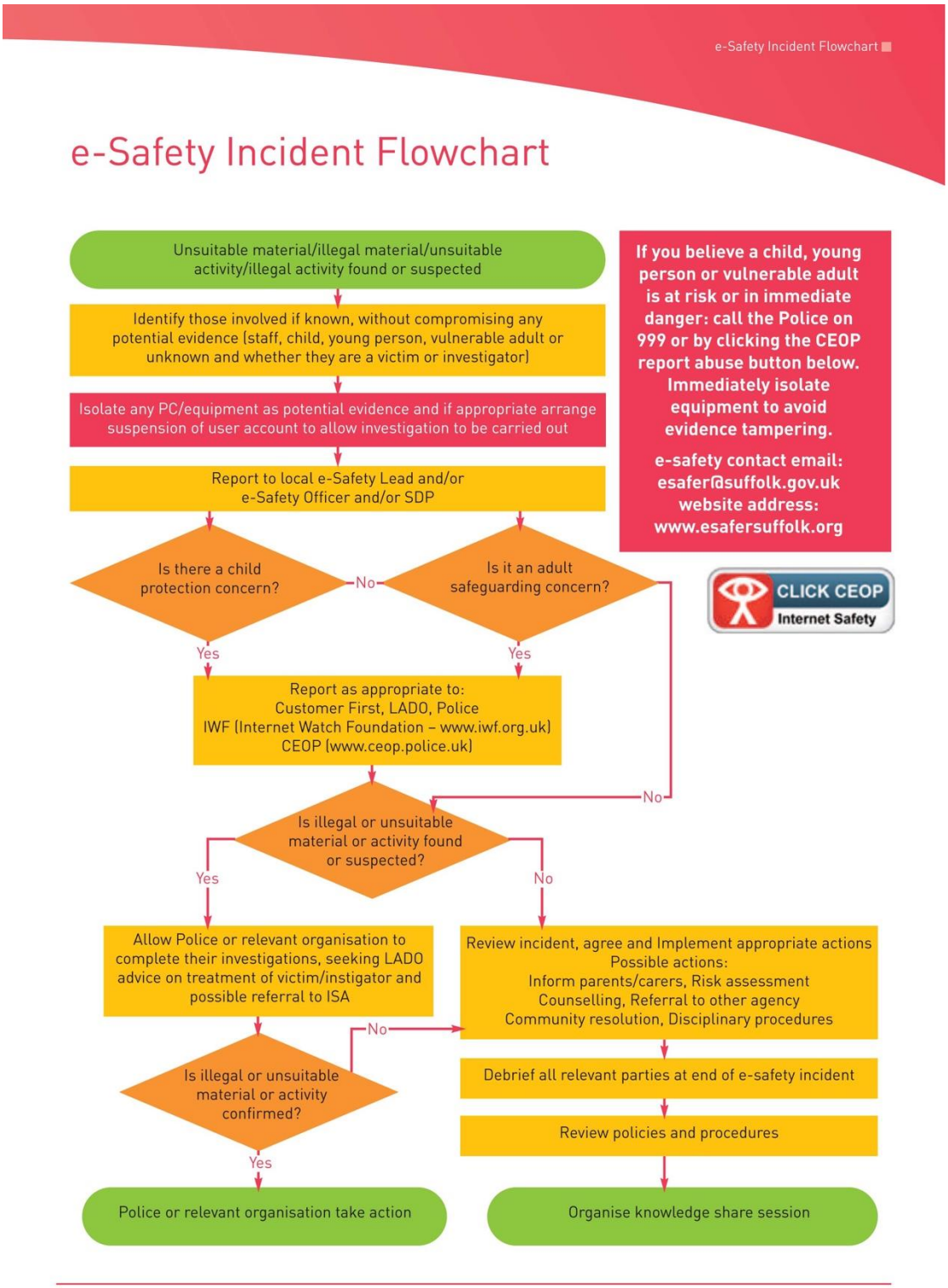
Wearable Technology

Wearable technology (such as GPS watches) is increasingly being used in schools to promote and further learning. At our School, we have utilised GPS watches. The School tries to balance the implications of using such devices, for example, the potential ability of hackers to track the pupil wearing them, with the benefit for the wearer. Presently, wearable devices are not allowed to be connected to the School's wireless network. This will be reviewed where it is deemed necessary and the correct safety measures can be ensured. The technician will monitor this situation.

Policy Review

This policy will be reviewed by the Online Safety Lead annually.

Appendix 1: Online Safety Flow Chart



Appendix 2:

Bures Primary School
Acceptable Use Agreement for Staff, Governors and Visitors.

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.

- I know that I must only use the school equipment in an appropriate manner and for professional uses.
- 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.
- I know that images should not be inappropriate or reveal any personal information of children and young people if uploading to the internet.
- I have read the Online Safety Policy so that I can deal with any problems that may arise, effectively.
- I will report accidental misuse to the Online Safety Lead.
- I will report any incidents of concern for a child or young person's safety to the Headteacher, Senior Designated Person or Online Safety Lead in accordance with procedures listed in the Online Safety Policy.
- I know who the Senior Designated Person is at Bures School.
- I know that I am putting myself at risk of misinterpretation and allegation should I contact children and young people via personal technologies, including my personal e-mail. I know I should use the school e-mail address and phones (if provided) and only to a child's school e-mail address upon agreed use within the school.
- I know that I must not use the school system for personal use unless this has been agreed by the Headteacher and/or Online Safety Lead.
- I know that I should complete virus checks on my laptop and memory stick or other devices so that I do not inadvertently transfer viruses, especially where I have downloaded resources.
- I will ensure that I follow the Data Protection Act 1998 and have checked I know what this involves.
- 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.

- I will adhere to copyright and intellectual property rights.
- I will only install hardware and software I have been given permission for.
- 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.
- I have been given a copy of the Online Safety Policy to refer to about all Online Safety issues and procedures that I should follow.

I have read, understood and agree with these Statements 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)…….

School ……

1839 † Bures School

Appendix 3:

Bures Primary School
Acceptable Use Policy for Young People

My Online Safety Agreement
This is my agreement for using the internet safely and responsibly at school.

- 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 or video-conference people I know in the real world or that a trusted adult has approved.
- Adults are aware when I use online tools such as video conferencing.
- 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 or that I will not include my full name with photographs.
- If I need help I know who I can ask and that I can go to www.thinkuknow.co.uk or the NSPCC for help, if I cannot talk to a trusted adult.
- If I see anything on the internet that makes me feel uncomfortable, I know what to do.
- If I receive a message sent by someone I don't know, I know to let a trusted adult know and take a screenshot of the message.
- I know I should 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.

Signed …… / ..... Dated.....
(Pupil and Parent/Carer)

Name.....(Printed) Year ……

Pupils

Incidents:	Refer to class teacher	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X	X	X	X	X	X	X	X
Unauthorised use of non-educational sites during lessons	X	X					X	
Unauthorised use of mobile phone / digital camera / other mobile device	X	X			X		X	
Unauthorised use of social media / messaging apps / personal email	X	X			X		X	
Unauthorised downloading or uploading of files	X	X		X			X	
Allowing others to access school network by sharing username and passwords	X			X			X	
Attempting to access or accessing the school network, using another student's / pupil's account	X			X			X	
Attempting to access or accessing the school network, using the account of a member of staff		X			X			X
Corrupting or destroying the data of other users	X	X		X				X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X		X			X
Continued infringements of the above, following previous warnings or sanctions		X	X		X			X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X		X				X
Using proxy sites or other means to subvert the school's / academy's filtering system		X		X	X		X	
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X	X	X		X	X
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X			X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		X						X

Staff / Governors/Visitors

Incidents:	Refer to line manager	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X	X		X	X			X
Inappropriate personal use of the internet / social media / personal email	X	X			X	X		
Unauthorised downloading or uploading of files	X				X	X		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X				X	X		
Careless use of personal data eg holding or transferring data in an insecure manner	X	X			X	X		
Deliberate actions to breach data protection or network security rules		X			X	X		X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X			X	X		X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X	X	X		X	X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils. Using a personal mobile device to photograph children.		X	X					X
Actions which could compromise the staff member's professional standing		X	X		X			X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X			X		X	
Using proxy sites or other means to subvert the school's filtering system	X				X	X	X	
Accidentally accessing offensive or pornographic material and failing to report the incident		X	X		X			
Deliberately accessing or trying to access offensive or pornographic material		X		X	X		X	
Breaching copyright or licensing regulations		X			X			X
Continued infringements of the above, following previous warnings or sanctions		X			X		X	X