Wetheringsett Church of England Primary School
office@wvcpschool.com
01449 766215

St Edmundsbury and Ipswich Diocesan Multi Academy Trust

E-Safety Policy

Our Vision

'Growing skills for life', we aim to provide children with all the skills they need – not just academic, to be successful, fully rounded individuals, ready for the next stage in their lives.

'**We value and cherish each child, supporting all to be successful. Our Christian values underpin everything we do.'**

Our Values

As part of our school aim of 'growing skills for life', we work to support our children as individuals. As a church school, promoting Christian values is an important part of this.
Our 6 core values are friendship, generosity, courage, compassion, thankfulness and perseverance.

Person Responsible:	**Headteacher**
Approval Body:	**Curriculum Committee**
Date of approval:	**Spring 2021**
Review date:	**Autumn 2023**

Signed as approved by the Chair of Governors/Committee: …….
Date: …….

1. **Introduction**

- ICT in the 21st Century is an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young

people with the skills to access life-long learning and employment.

- Information and Communications Technology covers a wide range of resources including web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:
    - Websites
    - E-mail, instant messaging and chat rooms
    - Social media, including Facebook and Twitter
    - Smart phones with text, video and/ or web functionality
    - Other mobile devices with web functionality
    - Gaming, especially online
    - Wearable technology
    - Smart TVs and streaming devices
    - Blogs and vlogs
    - Podcasting
    - Video broadcasting
    - Music & video downloading and other streaming

- Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies and that some have minimum age requirements, usually 13 years.

- At Wetheringsett C of E Primary School we understand the responsibility to educate our pupils on e-Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

- Both this policy and the Responsible Use Agreements (for all staff, governors, visitors, parents/carers & pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, tablets, whiteboards, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, smart phones, tablets, wearable technology and other mobile devices).

2. Monitoring

- The headteacher and any member of staff or outside organisation who the headteacher has authorised, may monitor, intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain school business related information; to confirm or investigate compliance with school policies, standards and procedures; to ensure the effective operation of school ICT; for quality control or training purposes; to comply with a Subject Access Request under the General Data Protection Act 2018, or to prevent or detect crime.

- Authorised staff may, without prior notice, also access the e-mail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.

- All monitoring, surveillance or investigative activities are conducted by authorised staff and

comply with the General Data Protection Act 2018, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

- It should be noted that personal communications using School ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

3. Links to other policies

This policy should be viewed in conjunction with the school's Behaviour Policy, Anti-Bullying Policy and Data Protection Policy.

- Acceptable Use Agreements are also in place for staff, governors, pupils and parents (see Appendix 5). E-Safety is also reference in the Volunteer's Code of Conduct.

4. Incident Reporting

- Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's eSafety Lead. Consideration should also be given as to whether the incident constitutes a data breach and thus whether procedures under the Data Protection Policy should be followed.

- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the e-Safety Lead/headteacher, depending on the seriousness of the offence the LA may also be informed and immediate suspension, possibly leading to dismissal and involvement of police for very serious offences could result.

- Procedures, as outlined in Appendix 1, 2 & 3 will be followed in the event of an eSafety incident. An incident log is kept by the e-safety coordinator. See Appendix 4.

5. Computer Viruses

- All files downloaded from the Internet, received via e-mail or on removable media such as a memory stick/USB must be checked for any viruses using school provided anti-virus software before being used.

- Staff should never interfere with any anti-virus software installed on school ICT equipment that they use .

- If anyone suspects there may be a virus on any school ICT equipment, they should stop using the equipment and contact their ICT support provider immediately. The ICT support provider will advise them what actions to take and be responsible for advising others that need to know.

- Staff should be vigilant of possible malicious emails and attachments and take advice before opening anything that appears suspicious.

- To reduce the likelihood of viruses/malware/spyware etc. automatically diabled extensions (such as Flash Player) should not be bypassed.

6. Disposal of Redundant ICT Equipment Policy

- All redundant ICT equipment will be disposed of through an authorised agency. A list of these is provided by SCC procurement service. This should include a written receipt for the item including an

acceptance of responsibility for the destruction of any personal data.

- All redundant ICT equipment that may have held personal data will have the data irretrievably destroyed. Or if the storage media has failed it will be physically destroyed. We will only use authorised companies who will supply a written guarantee that this will happen.

- Disposal of any ICT equipment will conform to:
  The Waste Electrical and Electronic Equipment Regulations 2006
  The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007

  The General Data Protection Act 2018

  Electricity at Work Regulations 1989

- The school will maintain a comprehensive inventory of all its ICT equipment including a record of disposal.

- The school's disposal record will include:
  - Date item disposed of
  - Authorisation for disposal, including:
    Verification of software licensing
    *Any personal data likely to be held on the storage media? **
    How it was disposed of eg waste, gift, sale
  - Name of person & / or organisation who received the disposed item

- Any redundant ICT equipment being considered for sale / gift will have been subject to a recent electrical safety check and hold a valid PAT certificate.

7. E-mail

- The school gives all staff and governors their own e-mail account to use for all school business as a work based tool. This is to protect staff and governors, minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed.

- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The school email account should be the account that is used for all school business.

- Under no circumstances should staff or governors contact pupils, parents or conduct any school business using personal e-mail addresses.

- The school requires a standard disclaimer to be attached to all staff e-mail correspondence, stating that, 'the views expressed are not necessarily those of the school or the LA'. The responsibility for adding this disclaimer lies with the account holder.

- All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper.

- Documents to parents should be sent in a form that cannot be edited eg pdf.

- Staff sending e-mails to individual pupils are advised to cc. the Headteacher.

- Groups of parents should be emailed using bcc to prevent 'reply all's. The headteacher should be copied into all staff emails to parents.

- However school e-mail is accessed (whether directly, through webmail when away from the office or on non-school hardware), all the school e-mail policies apply (See 17.c).

- Emails should not be re-directed to personal email addresses.

- Staff and governors should
    - check their email regularly
    - Activate their 'out-of-office' notification when away for extended periods
    - Never open attachments from an untrusted source

- All pupils from Y1 have their own individual school issued accounts. Accounts are deleted when the child leaves the school.

- All pupil e-mail users are expected to adhere to the generally accepted rules of etiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments.

- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail.

- Staff must inform (the eSafety Lead/ headteacher) if they receive an offensive e-mail.

- Pupils are introduced to e-mail as part of the computing curriculum.

- Staff should follow the guidance on the Data Protection Policy on sharing sensitive information electronically, including by email.

8. Equal Opportunities

Pupils with Additional Needs

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the school's eSafety rules.

However, staff are aware that some pupils may require additional support or teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of eSafety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of eSafety. Internet activities are planned and well managed for these children and young people.

9. Roles and Responsibilities

The headteacher and governors have ultimate responsibility to ensure that the policy and practices are

embedded and monitored. The E-Safety Lead in this school is the headteacher. It is the role of the eSafety Lead to keep abreast of current issues and guidance through organisations such as SCC, CEOP (Child Exploitation and Online Protection) and Childnet, ThinkUKnow and the NSPCC.

Governors are regularly updated about E-safety by the headteacher as part of Safeguarding section of the headteacher's termly report. All governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's Acceptable Use Agreements for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community.

10. E-Safety in the Curriculum

- The school has a framework for teaching internet skills in Computing lessons through 'Cyberwisdom' units.
- In addition, educating pupils about the online risks that they may encounter outside school is done informally when opportunities arise.
- Pupils are taught about copyright, respecting other people's information, safe use of images and other important areas through discussion, modeling and appropriate activities.
- Pupils are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. As they move through the school, pupils are also made aware of where to seek advice or help if they experience problems when using the internet and related technologies at an age appropriate level; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Cybermentors, Childline or CEOP report abuse button.
- Pupils are taught to critically evaluate materials and learn good searching skills, including how to differentiate between safe and unreliable sources of information, through cross curricular teacher models, discussions and via the Computing curriculum.

11. E-Safety Skills Development for Staff

- New staff receive information on the school's responsible use agreements as part of their induction.
- All staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context of eSafety and know what to do in the event of misuse of technology by any member of the school community (as outlined in Section 4).

12. Internet Access

- The school provides pupils with supervised access to internet resources.
- Staff will preview any recommended sites before use.
- All users must observe copyright of materials from electronic resources.
- Members of the school community must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise the intended restricted audience.

- They should not reveal names of colleagues, pupils, others or any other confidential information acquired through their job on any social networking site or other online application.
- On-line gambling, and similar activities, are not allowed.
- It is at the headteacher's discretion as to what internet activities are permissible for staff and pupils and how this is disseminated.
- School internet access is controlled through the web filtering service surfprotect.
- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the e-safety coordinator or teacher as appropriate.
- It is the responsibility of the school, by delegation to the network manager, to ensure that anti-virus protection is installed and kept up-to-date on all school machines.
- Staff should only use the encrypted USB memory stick provided by the school.
- Pupils and staff are not permitted to download programs (including Apps) on school based technologies without seeking prior permission from the headteacher.
- If there are any issues related to viruses or anti-virus software, the network manager (support@debenhamhigh.co.uk) should be informed.

13. Managing Other Technologies

- All pupils are advised to be cautious about the information given by others on such websites, for example users not being who they say they are.
- Pupils are taught to be cautious about placing images of themselves (or details within images that could give background details) on such websites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- Pupils are always reminded to avoid giving out personal details on websites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests).
- Our pupils are advised to set and maintain their online profiles to maximum privacy and deny access to unknown individuals.
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts and information online.
- Our pupils are asked to report any incidents of Cyberbullying to the school.
- Staff may only create blogs, wikis or other online areas in order to communicate with pupils using the school learning platform or other systems approved by the headteacher.

14. Parental Involvement

- Parents/carers are asked to read through and sign acceptable use agreements in conjunction with

their child on admission to the school.

- We regularly discuss eSafety with parents/ carers and seek to promote a wide understanding of the benefits of new technologies, together with the associated risks.

- Parents/carers are asked for consent for use of their child's image (see Data Protection Policy)

- The school disseminates information to parents relating to eSafety where appropriate in the form of

  Information evenings
  Posters
  School website
  Newsletter items

15. Use and Storage of Images and Videos

With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images or video by staff and pupils **with school equipment.**

- Staff are not usually permitted to use personal digital equipment, such as mobile phones and cameras, to record images or video of pupils, this includes when on school trips.

- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images or video of pupils, staff and others without advance permission from the Headteacher.

- Pupils and staff must have permission from the Headteacher before any image or video can be uploaded for publication.

- Images and video should be immediately deleted from memory cards and they should not be stored on hardware unless it is deemed that it will be needed in future.

- Images and video of children are deleted off all hardware within a year of the child leaving at the end of Year 6.

- Before sharing or posting student images or videos online, staff should check whether the school has parental consent for this.

- Only those authorized to by the headteacher may upload images or video onto the school website.

- Permission to use images or video of all staff who work at the school is sought on induction and a copy is located in the personnel file.

16.Webcams, CCTV and Video Conferencing

- The school does not use CCTV.

The school has no standalone webcams, but much of our hardware has built in cameras.

Consent is sought from parents/carers and staff on joining the school, in the same way as for all images for the online use of webcams.

Misuse of the webcams by any member of the school community will result in sanctions.

Permission is sought from parents and carers for video conferences on admission.

All pupils are supervised by a member of staff when video conferencing.

Approval from the headteacher is sought prior to all video conferences within school.

Digital records are to be kept of video conferences (where possible) and software/programmes that enable safe recording are preferred. These recordings should be treated in line with the rest of this policy.

To avoid any breach of personal privacy, all those partaking in a video conference from home should choose a private, suitable background for their video conference - using an auto-generated image or blur filter when this is not possible - dress appropriately, and use headphones for privacy.

17. School ICT Equipment including Portable & Mobile ICT Equipment & Removable Media

a. School ICT Equipment

- As a user of the school ICT equipment, the user is responsible for their activity.
- The school logs ICT equipment issued to staff and records serial numbers as part of the school's inventory.
- Visitors to the school are allowed to use the school's wireless ICT facilities with permission from the headteacher.
- All ICT equipment must be kept physically secure (see Data Protection Policy).
- Users should not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990.
- It is imperative that users save data on a frequent basis and it is recommended that this is done by uploading onto the school's online network (Google Drive). Users are responsible for the backup and restoration of any of their data that is not held on this.
- Personal or sensitive data should not be stored on the local drives of desktop PC, laptop, USB memory stick or other portable device without encryption. An encrypted USB stick is provided for all teaching staff. This must be stored securely. It is recommended that it is attached to the individual's name badge lanyard.
- A 5 minute time locking screensaver should be applied to all non-pupil machines.
- On termination of employment, resignation or transfer, all ICT equipment should be returned to the school. Staff must also provide details of all their system logons so that they can be disabled.
- It is the staff member's responsibility to ensure that any information accessed from their own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person.
- All ICT equipment allocated to staff must be authorised by the headteacher.

All redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA).

b. Portable & Mobile ICT Equipment

- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of the car before starting a journey.

- Staff must ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades.

- The installation of any applications or software packages must be authorised by the headteacher and fully licensed.

- In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight.

- Portable equipment must be transported in its protective case if supplied.

c. Personal Mobile Devices

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal accounts eg text. If the staff member knows a family out of school and may therefore be contacting them socially, they should inform the headteacher of this relationship.

- Staff personal devices may be connected to the school's wifi.

- Personal mobile devices should be kept in the staffroom during school hours.

- Pupils are allowed to bring personal mobile devices/phones to school but must hand them over to staff for safekeeping in the school safe until the end of the school day.

- The school is not responsible for the loss, damage or theft of any personal mobile device.

- The sending of inappropriate text messages between any member of the school community is not allowed.

- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community.

- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

18. Servers

The office server is used for storage of administrative data.

This is password protected and access limited to admin, finance and senior school staff.

Data is backed up regularly using Suffolk County Council's remote back up is used which is securely encrypted.

19. Social Media, including Facebook and Twitter

- Staff are permitted to access their personal social media accounts using school equipment during their break times.

- Staff are able to set up social media accounts, using their school email address, in order to be able to teach pupils the safe and responsible use of Facebook or other applications.

- Pupils are not permitted to access their social media accounts whilst at school.

- Staff, governors, pupils, parents and carers are regularly provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others.

- Staff, governors, pupils, parents and carers are aware that the information, comments, images and video they post online can be viewed by others, copied and stay online forever.

- Staff, governors, pupils, parents and carers are aware that their online behaviour should at all times be compatible with UK law.

20. Systems and Access

- All users are responsible for all activity on school systems carried out under any access/account rights assigned to them, whether accessed via school ICT equipment or their own PC.

- They should not allow any unauthorised person to use school ICT facilities and services that have been provided to them.

- They must only use their personal logons, account IDs and passwords and not allow them to be used by anyone else.

- They must keep their screen display out of direct view of any third parties when they are accessing personal, sensitive, confidential or classified information.

- Users must ensure they lock their screen before moving away from their computer during their normal working day to protect any personal, sensitive, confidential or otherwise classified data and to prevent unauthorised access.

- They should ensure that they logoff from the PC completely when they are going to be away from the computer for a longer period of time.

- It is imperative that users do not access, load, store, post or send from school ICT any material that is, or may be considered to be, illegal, offensive, libellous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the school or may bring the school or SCC into disrepute. This includes, but is not limited to, jokes, chain letters, files, emails, clips or images that are not part of the school's business activities; sexual comments or images, nudity, racial slurs, gender specific comments, or anything that would offend someone on the basis of their age, sexual orientation, religious or political beliefs, national origin, or disability (in accordance with the Sex Discrimination Act, the Race Relations Act and the Disability Discrimination Act).

- Any information held on school systems, hardware or used in relation to school business may be subject to The Freedom of Information Act.

- Where necessary, users should obtain permission from the owner or owning authority and pay any relevant fees before using, copying or distributing any material that is protected under the Copyright, Designs and Patents Act 1998.

21. Telephone Services

- Staff may make or receive personal telephone calls provided:
    1. They are infrequent, kept as brief as possible and do not cause annoyance to others
    2. They are not for profit or to premium rate services
    3. They conform to this and other relevant SCC and school policies.

- School telephones are provided specifically for school business purposes and personal usage is a privilege that will be withdrawn if abused

Staff should be aware that the laws of slander apply to telephone calls. Whilst a telephone call may seem to have a temporary and private existence it still qualifies as admissible evidence in slander law cases

22. Writing and Reviewing this Policy

- There will be on-going opportunities for staff to discuss with the eSafety coordinator any eSafety issue that concerns them.

- There will be on-going opportunities for staff to discuss with the SIRO/AIO any issue of data security that concerns them.

- This policy will be reviewed every 3 years and amended if new technologies are adopted and/or central government change the orders or guidance in any way.

If the incident **did not** involve **any illegal activity** then follow this flowchart.

Appendix 1 –Responding to an Iilegal eSafety Incident Flow Chart

If member of staff has:
1. Behav… …d,

If you are not sure if the incident has any illegal aspects contact immediately for advice either:
School HR (staff)
Local Safer Neighbourhood Officer

- R… …e incident is accidental or deliber…

- Inform police and the Northern Area Education Office **01502 405293**. Follow any advice given by the Police otherwise
- Confiscate any laptop or other device and if related to school network disable user account
- Save **ALL** evidence but **DO NOT** view or copy. Let the Police review the evidence

If a pupil is involved inform Customer First **0800 800 4005**
If a member of staff, contact the Local Authority Designated Officer (LADO) on **01473 263122**

Following an incident the eSafety Coordin… and/or Headteacher will need to decide… if the incident involved any illegal activi…

Incident could be
- Using another person's user name and password
- Accessing websites which are against school policy e.g. games, social networks
- Using a mobile phone to take video during a lesson
- Using the technology to upset or bully (in extreme cases could be illegal)

…reme cases of …yberbullying
Promoting ill… …gious

Was illegal material or activity found or suspected?

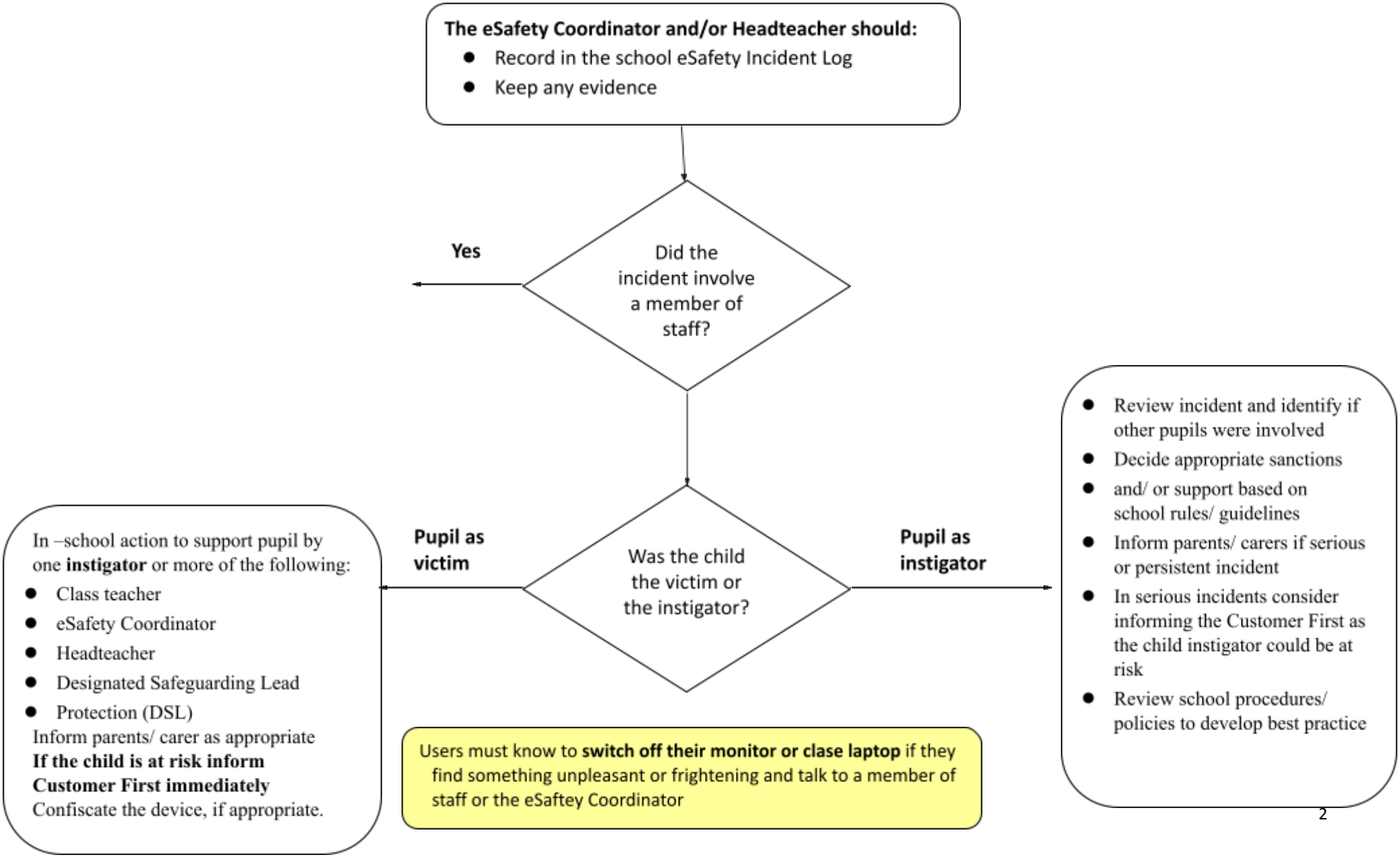
Yes

No

If the incident **did not** involve **any illegal activity** then follow the next flowchart relating to non-illegal incidents

Users must know to **switch off their monitor or clase laptop** if they find something unpleasant or frightening and talk to a member of staff or the eSaftey Coordinator

Appendix 2 –Responding to an eSafety Incident Flow Chart



Appendix 3 - Responding to an eSafety Incident where Staff are Victims

All incidents should be reported to the Headteacher and/or Chair of Governors (if the headteacher is involved) who will:

- Record in the school eSafety Incident Log
- **Keep any evidence – printouts and/ screen shots**
- Use the 'Report Abuse' button, if appropriate
- Consider involving the Chair of Governors and /or reporting the incident to the Governing Body

Parents/ carers as Instigators

Follow some of the steps below:

- Contact the person and invite into school and discuss using some of the examples below:
  - You have become aware of
  - discussions taking place online …
  - You want to discuss this…
  - You have an open door policy so disappointed they did not approach you first
  - They have signed the Home
  - School Agreement which clearly states …
  - Request the offending material be removed.
- If this does not solve the problem:
  - Consider involving the Chair of Governors
- You may also wish to send a letter to the parent

Staff as instigators

Follow some of the steps below:

Contact Schools HR for initial advice and/ or contact the Northern Area Education Office **01502 405293.**

In all serious cases this is the first step.

Contact the member of staff and request the offending material be removed immediately, (**in serious cases you may be advised not to discuss the incident with the staff member**)

Refer to the signed ICT Responsible Use Agreement, Staff Code of Conduct and consider if this incident has an impact on the Contract of Employment of the member of staff.

Further contacts to support staff include:

- SCC Single Point of Contact (Kathryn Day)
- Schools HR
- School Governance
- Suffolk Police

The HT or Chair of Governors can be the single point of contact to coordinate responses.

- The member of staff may also wish to take advice from their union

Pupils as instigators

Follow some of the steps below:

- Identify the pupils involved
- Ask pupil to remove offensive material. Refer to the signed Responsible Use Agreement.
- If the perpetrator refuses to remove the material and is under 13 contact the social network who will close the account
- Take appropriate actions inline
- With school policies/ rules Inform parents/ carers if serious or persistent incident

For serious incidents or further advice:

- Inform your Local Police Safer
- Neighbourhood Team
- If the child is at risk talk to your
- school DSL (Designated Safeguarding Lead) who may decide to contact the LADO

Appendix 4 – eSafety Incident Log

Wetheringsett Primary School eSafety Incident Log

Details of ALL eSafety incidents to be recorded by the eSafety Lead. This incident log will be monitored termly by the Headteacher or Chair of Governors. Any incidents involving Cyberbullying may also need to be recorded elsewhere

Date & time	Name of pupil or staff member	Male or Female	Room and computer/ device number	Details of incident (including evidence)	Actions and reasons

Appendix 1 – Acceptable Use Agreements

Pupil Acceptable Use Agreement

- I will only use ICT in school for school purposes.
- I will only use my class email address or my own school email address when emailing.
- I will only open email attachments from people I know, or who my teacher has approved.
- I will not tell other people my passwords.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- I will not give out personal information such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community
- If anyone posts anything online or sends me anything that makes me upset or uncomfortable, I will tell my teacher.
- I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my eSafety.
- I will not upload text images, videos etc to a website without permission from a teacher.
- I will not electronically distribute pictures or videos of staff or pupils without permissions
- I understand that the school can respond to online bullying or other e-Safety incidents, even if they take place outside of school.

Dear Parent/ Carer,

ICT including the internet, email and mobile technologies, etc has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.

Please read and discuss these eSafety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact Vicky Doherty, eSafety Lead.
Yours sincerely,

Mrs Sam Sheeran
Head of School

✂ _____

Acceptable Use Agreement

We have discussed this and …….(child name) agrees to follow the eSafety rules and to support the safe use of ICT at Wetheringsett C of E Primary School.

Parent/ Carer Signature …….

Child's Signature ……..

Class …….. Date ……

Parent/Carers' Acceptable Use Agreement

Technology is an increasingly important part of everyday life and offers convenient and effective way of communicating, including between home and school.

We take online safety very seriously at school and have robust policies and procedures in place. The following documents outline our approach and the steps we take to keep everyone safe and to ensure there is a shared understanding of acceptable and responsible behaviour:

- *Responsible use agreements for children, staff and governors*
- *E-safety and data protection policies*
- *Anti-bullying Policy*
- *Safeguarding Policy*
- *Staff, volunteer and governor Codes of Conduct*
- *Consent forms when children start school*

We also ask parents to read and sign this Parents' Acceptable Use Agreement so they have all the information and advice they need on what is and isn't acceptable and an agreement on this is in place from the start.

Parent/Carer's Acceptable Use Agreement

Use of Digital / Video Images

Parents/carers are welcome to take videos and digital images of their children at school events for their own personal use. To respect everyone's privacy (and in some cases protection), images which contain other children should not be published or made publicly available on social networking sites.

Use of Social Media

Social media is a great way to share news and views and celebrate family members' achievements, including when your children have taken part in school events that are open to the public. However, please do not name others (children or adults) relating to school events and see above for guidance on the use of images.

If you have any concerns about the school, in line with our Complaints Policy, we ask that you follow the proper procedures and raise it with the relevant member of staff rather than posting your concerns on social media. Any form of misuse directed at the school, its employees, the pupils or anyone associated with the school will be taken very seriously. If any illegal activity or content is suspected the school will inform the necessary authorities.

Online Behaviour at Home

We highly recommend parents supervise their children's online activities when primary aged and that families discuss and set up home internet agreements. There are some great resources to support this: http://www.safekids.com/family-contract-for-online-safety//, http://www.childnet.com/blog/family-agreement.

The online CEOP (Child Exploitation and Online Protection) Centre provides excellent guidance and a means of reporting abuse or unsuitable materials. A CEOP browser safety tool can be downloaded and added to most browsers (eg Chrome, Internet Explorer), providing instant access to support.

We recommend that you encourage open discussion with your child about anything that may concern them when they are online. It is also worth considering that the understandable instinct to ban children from the internet when they have told you about a concern can be a deterrent to future open communication.

Parents should also be aware that social media accounts such as instagram, facebook and kik have minimum age requirements of at least 13 so primary age children should not have accounts.

It is a good idea to find out how to block 'friends' from online gaming groups (eg PS4), messaging services (eg imessage) and social media accounts before your child starts using them so you are able to act quickly and confidently if things do go wrong.

We ask that parents inform the school of any activity or concerns that they become aware of that the school should be aware of or could help to address through teaching.

Contacting Staff

We welcome email as a way for parents and staff to communicate easily with with each other. All staff have email addressing that are their name and the school domain name (eg *mrs.doherty*, followed by *@wvcpschool.com*). However, please remember that teachers have a high workload and do a very pressured job. Excessive emails from parents can add to this workload and pressure so please consider this when contacting them.

Teachers are also very busy during the day and are not able to access emails when teaching. They are also entitled to 'down time' when they are at home in the evenings. Emails may therefore not always be picked up quickly and a quick response may not always be possible.

Absence and on-the-day changes to collection **must** be communicated by phone or in person, not email.

Parent/Carer's Acceptable Use Agreement

I/We have read and accept the Parent/Carer's Acceptable Use Agreement

Child/Children's name(s) _____

Signed _____

Date _____

Please indicate whether you would be interested in attending a session for parents on online safety

Yes *No*

Staff Acceptable Use Agreement

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the headteacher who is the school's eSafety Lead.

All staff should ensure they are familiar with the school's Data Protection Policy and E-Safety Policy and comply with these.

Data Protection:

I will ensure that:

- school portable electronic devices, such as laptops and hard drives are stored securely:
  For example
  - locked in cupboard overnight if left in school
  - not left for longer than absolutely necessary in vehicles
  - kept within sight when in public places
- personal data is not in the view of others when being used
- my computer screens is locked when unattended and set to autolock after 5 minutes;
- personal data (including assessment data, SEN information, pupil premium information) is only held on the school network (google drive) or a school issued device (laptop, USB memory stick or other removable media) which is encrypted (NB - teacher laptops do not have encryption). I will not store such documents on any personal equipment
- I only use the encrypted USB memory stick provided by the school and keep this secure (recommended that this is on your name tag)
- passwords are not shared
- passwords comply with the complexity requirements, are changed regularly and different passwords are used for separate systems and devices
- personal data is only shared where necessary and in accordance with school policy, internally by sending a link to a document on Google Drive, externally using password protection, phoning through the password to the recepient
- if I access my school email account on my phone, it has a passcode and notification settings are set so that no content of the message is displayed on the lock screen

School Protocols

- I will use 'bcc' when I email parent groups (class/year groups/all parents) and copy in the headteacher.
- I will provide the office manager with a copy of my laptop password to be kept in a sealed envelope in the school safe.
- I will follow the school's reporting procedure in the event of a data breach (see Data Protection Policy), if I receive an offensive/potentially illegal email (see e-Safety Policy) or accidentally access inappropriate materials
- I will avoid email contact with individual children. If correspond**ence is received from a child, for transparency, I will forward this to the headteacher and copy the headteacher into any reply.**
- I will share documents internally using a link to Google Drive, rather than an attach**ment wherever possible**
- I will check my emails regularly and activate my 'out of office' notification if away for an extended period
- I will not open for forward any suspicious looking emails or attach**ments and report them to the headteacher**
- I will keep my mobile phone in the in the staffroom during school hours
- I will only take, store and use mages of pupils and/or staff for professional purposes in line with school E-safety Policy and with written consent of the parent, carer or staff member. I will not distribute images outside the school network without the permission of the parent/carer, member of staff AND Headteacher.

Responsible Use

- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
- I will only use the approved, secure email system(s) for any school business.
- I will not install any hardware or software without permission of the headteacher

- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to the Headteacher.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community
- I will not pass on personal, sensitive or confidential information acquired through my role or post it on any social networking site or other online application.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute. **I will support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.**
- I understand this forms part of the terms and conditions set out in my contract of employment.

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school

Signature ……..……...…….…… Date ……

Full Name ……..(printed)

Job title ……..

Governors Acceptable Use Agreement

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all governors are aware of their responsibilities when using any form of ICT. All governors are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the headteacher who is the school's eSafety Lead.

All governors should ensure they are familiar with the school's Data Protection Policy and e-Safety Policy and comply with these.

- I will only use the approved, secure school email system for any school governor business
- I will not forward/automatically redirect emails to any other email account
- I will not download and save governor documents to the harddrive of any personal device
- My school email account will be password protected. The hardware I use will need a password each time it is accessed OR my email account will require a password each time it is used
- I will ensure that sensitive data is not in the view of others when being used
- I will share documents internally using a link to Google Drive, rather than an attachment wherever possible
- if I access my school email account on my phone, I will ensure it has a passcode and that notification settings are set so that no content of the message is displayed on the lock screen
- I will ensure that all electronic communications with members of the school community are compatible with my role as a governor
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute
- I will not pass on personal, sensitive or confidential information acquired through my role on any social networking site or other online application

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school

Signature ……..…….. Date ……

Full Name ……..(printed)