Burstwick Community Primary School

E-safety Policy

"BURSTWICK: Small School. Big Hearts. Where Learning Comes Alive."

At Burstwick Community Primary School, our children thrive, develop and master their independence and confidence in a busy and enthusiastic learning environment.

Within our school, our children have a strong voice, feel cared for, supported and are part of the Burstwick family.

At Burstwick Community Primary School, we live by our core values. These values support the development of the whole child as a reflective learner within an enthusiastic and focused atmosphere.

***CORE VALUES: B**elievers, **U**nique, **R**esilient, **S**afe, **T**olerant, **W**orthy, **I**ndependent, **C**reative, **K**ind-hearted.*

*We are **BURSTWICK!***

Statement:

This policy has been developed to ensure that all stakeholders at Burstwick Community Primary School works to ensure safeguarding and promotes the welfare of children and young people.

Aims:
We aim to put effective management systems in place to maximise the education and social benefits obtained from ICT use whilst minimising the risks. This policy relates to other policies including those for ICT, behaviour and for child protection.

Teaching and learning
Internet Access

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.
- Our internet provision will be filtered using the LA mediated filtering system.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils, and use will enhance learning
- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
- Pupils will be shown how to publish and present information to a wider audience.
- Pupils will be taught how to evaluate Internet content and the school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught the importance of cross-checking information before accepting its accuracy.
- Pupils will be taught how to report unpleasant Internet content.

E-mail & Social networking/personal publishing

- **When available**, pupils may only use approved e-mail accounts on the school system.

This policy will be updated with guidance if school provided emails are made available to pupils or if personal publishing is incorporated into the curriculum.
Published content and the school web site

- Staff or pupil personal contact information will not be published. The contact details given online should be the school office.

- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Photographs that include pupils will be selected carefully so that individual pupils cannot be identified.
- Pupils' names may be used in association with photographs anywhere on the school preferred communication method, e.g. DOJO. However, publications with children's names are available on the website with parental permission. In BCPS, we prefer not to publish children's names on wider social media sites.
- Pictures and work will be shown on the website as part of our method of sharing children's success.
- Parents will be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

Managing videoconferencing & webcam use

- When available, videoconferencing and webcam use will be appropriately supervised for the pupils' age. Video conferencing equipment will always be shut off when not in use.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- Whilst the transfer of data from home to school is inevitable, sensitive or personal data will not be taken home unless it is on an encrypted, password protected device.
- Logins and passwords should be kept private.
- Computers will be locked when not in use. (Ctrl + Alt + Del)

Procedures

- The School ICT system's security will be reviewed regularly.
- Virus protection will be updated regularly.
- Acceptable use posters will be displayed around the school.
- The school will work in partnership with parents, the LA, DES and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- The school will adopt the latest DfE guidance for Filtering & Monitoring. This update was introduced in March 2023, and has formed a large part of the Keeping Children Safe in Education (KCSiE) 2026.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the ICT co-ordinator and the E-Safety Coordinator informed (Reporting sheet and Protocol Appendix 1,2,3). A copy of which will be on the Safeguarding Board.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. The school cannot accept liability for any material accessed, or any consequences of Internet access.
- The school should audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.
- E-Safety training will be embedded within the ICT scheme of work and the Personal Social and Health Education (PSHE) curriculum.

- E-Safety briefings and materials will be made available to parents.
- Pupils will be taught how to block someone online or report them using the CEOP button.
- Discretion and professional conduct is essential.
- No member of staff should engage in direct communication (in or out of school) of a personal nature with a pupil who is not a member of their direct family, by any means, for example (but not limited to) SMS text message, email, instant messaging or telephone. Should special circumstances arise where such communication is felt to be necessary, the agreement of a line manager should be sought first and appropriate professional language should always be used.
- Cyber-bullying will be dealt with using the school's Anti-Bullying Policy and/or the school's Behaviour for Learning Policy; and is seen as a serious offence.

Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with School child protection procedures.
- Pupils and parents will be informed of consequences for pupils misusing the Internet.

Enlisting parents' and carers' support

- Parents' and carers' attention will be drawn to the School E-Safety Policy in newsletters, the school brochure and on the school Web site.

The school will ask all pupils and staff to sign the relevant agreements when children are admitted.

Filtering & Monitoring

Schools must provide a safe environment to learn and work, including when online. Filtering and monitoring are both important parts of safeguarding pupils and staff from potentially harmful and inappropriate online material. Clear roles, responsibilities and strategies are vital for delivering and maintaining effective filtering and monitoring systems. It is important that the right people are working together and using their professional expertise to make informed decisions.

Governing bodies have overall strategic responsibility for filtering and monitoring and need assurance that the standards are being met. To do this, the Governing Body should identify and assign:

• A member of the senior leadership team and a governor, to be responsible for ensuring these standards are met
• The roles and responsibilities of staff and third parties, for example, external service providers

- The designated member of staff with responsibility for e-safety is Jake Penn
- The designated member of staff with strategic responsibility for e-safety is Ian Cutts
- The designated Governor with strategic responsibility for e-safety is Dominic Boynton

The senior leadership team are responsible for:

• Procuring filtering and monitoring systems
• Documenting decisions on what is blocked or allowed and why
• Reviewing the effectiveness of your provision
• Overseeing reports

They are also responsible for making sure that all staff:

• Understand their role
• Are appropriately trained

• Follow policies, processes and procedures
• Act on reports and concerns

Senior leaders will work closely with Governors, the DSL and IT service providers in all aspects of filtering and monitoring. Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL will work closely together with IT service providers to meet the needs of our setting.

The DSL (Ian Cutts) will take the strategic responsibility for safeguarding and online safety, which will include overseeing and acting on:
• Filtering and monitoring reports
• Safeguarding concerns
• Checks to filtering and monitoring systems

The IT service provider should have technical responsibility for:

• Maintaining filtering and monitoring systems
• Providing filtering and monitoring reports
• Completing actions following concerns or checks to systems

The IT service provider should work with the senior leadership team and DSL to:

• Procure systems
• Identify risk
• Carry out reviews
• Carry out checks

Safeguarding

The school is committed to safeguarding and promoting the welfare of all children and staff. We expect all staff and volunteers to share this commitment. Through the construction and writing of policies, we share our commitment; and through our curriculum provision, safeguarding is taught both explicitly (directly) and implicitly (indirectly).
We believe that all children have the right to learn in a supportive, caring and safe environment, which includes the right to protection from all types of abuse. Staff are vigilant for signs of any child in distress and we are confident about applying our safeguarding procedures to avert and alleviate any problems.

Monitoring and Review

Burstwick Community Primary School's e-Safety Policy is monitored regularly by the Senior Leadership Team (SLT) and E-Safety Coordinator, who report to the governors about its implementation and effectiveness. Governors are kept informed of any significant changes via the termly Headteacher's Report.

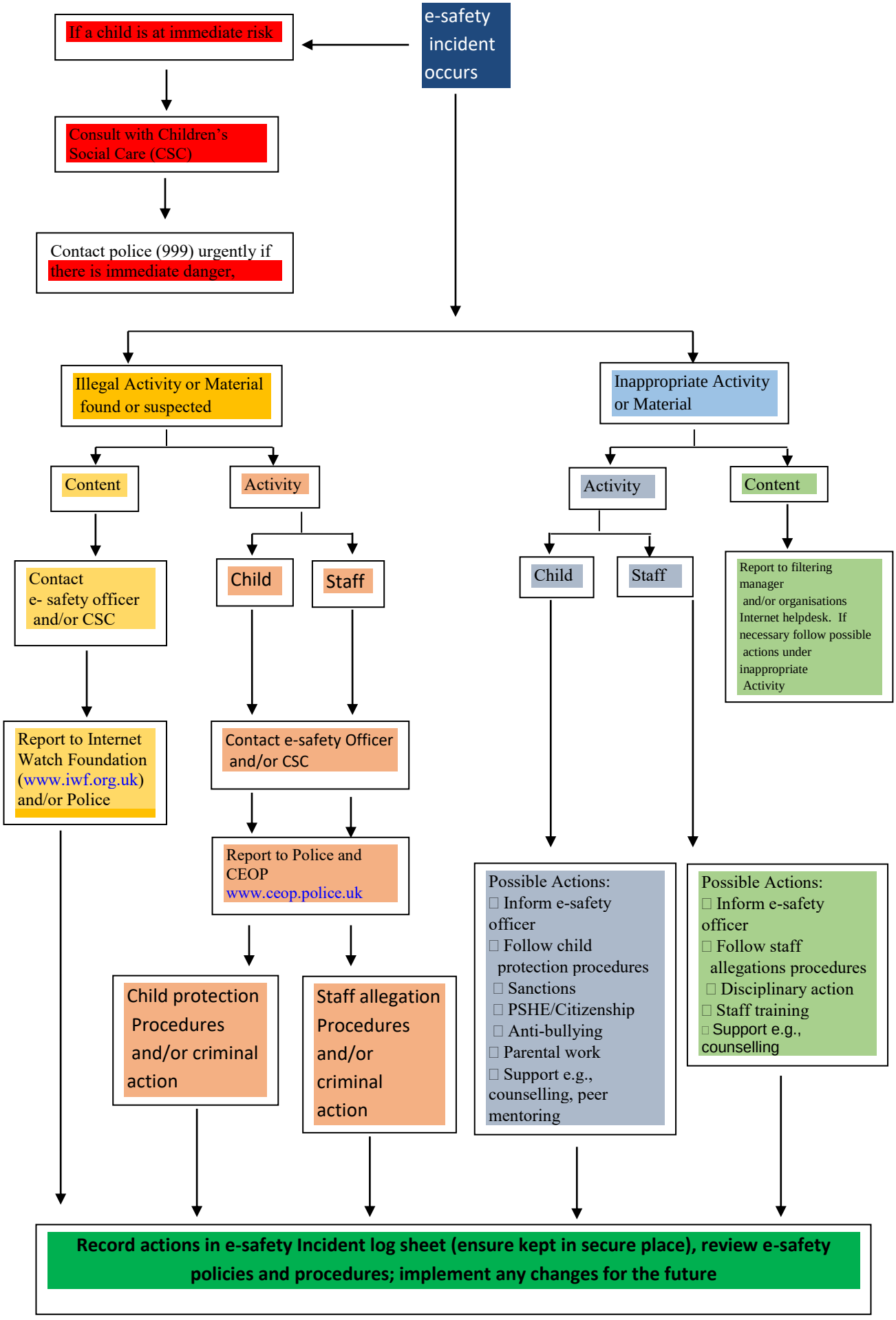
This Policy will be reviewed at least once every two years as a minimum, or if directives dictate change, through discussion with all staff and Governors.

Headteacher: ***Ian Cutts*** Chair of Governors: ***Andy Johnson***

Signed: Signed:

Date: Date:

Burstwick Primary School



Burstwick Primary School

e-Incident Log Sheet 1 – "member of staff identifying incident" – front cover

To be completed by the member of staff identifying the incident

Date of identification:		Date of incident (if different):	
Time of identification:		Time of incident (if different):	

Duration of incident:		Do you know if repeat victim?	yes	no	unsure

Description of the e-Safety incident:
(please give as much information as you are able – use the prompts overleaf in the guidance)

Description of information recorded or secured **(please refer to legal guidance overleaf)**	Yes	No
Have files, audio/text/images been recorded and secured? Has any computer or other technology including phones been secured?		

If yes, how and where, who by and when?

What actions were taken, and by whom? *Give details of agencies informed and contact person within those agencies.*

Name of person completing this form:	
Organisation:	
Date:	Signature:

Send this form immediately to the person with responsibility for child protection within your organisation

e-Incident Log Sheet 1 – "member of staff identifying incident" – guidance

Date and Time section:

Please complete all sections, if you don't know the exact day or time of the incident, please write 'unknown'

Description of the e-safety incident:

It is vital that all details you know are recorded, including how the information became known to you and from whom. If there is insufficient space on the form, please use additional sheets, but ensure that they are firmly attached and a note clearly identifies additional sheets used. Include detail of specific services or websites used if known (e.g., chat room, instant messenger); e-mail addresses; usernames etc. Give full details of real names and e-mail addresses etc where known. Some prompts to assist you could be: How was the incident identified? Who was involved and how do you know this? Why do you have concerns?

Description of information recorded or secured

Legal guidance for those reporting e–Safety incidents that involve a criminal offence

POWERS

If **any person** has reasonable grounds to believe that an offence IS being committed, then they may **detain the person (offender only)** and **secure any evidence** of the offence (including property). This would include the property of a victim or offender. Once evidence is secured the Police may then seize the property under the Police & Criminal Evidence Act 1984.

Offences committed via computers/laptops/mobile phones.

In these situations the securing of information **must be carried out in a specific way** in order to obtain the best evidence possible for the police and other law enforcement agencies. When a computer is turned on or on standby it should be **left exactly as it is**; in order to allow a trained seizure officer to attend. In all cases; attempts should be made to **record in note form** any details that can be seen on the screen. **DO NOT follow any links or change any pages**.

Information that should be noted if on screen:

o Website address.
o Email addresses of sender and recipient.
o Dates and Times.
o User names.
o Mobile phone numbers.
o Any profile information.
o Any text from chat conversations.

If a request for inappropriate behaviour is made on MSN, FACEBOOK, any chat forum or social networking site. **DO NOT DELETE or interfere with the offending account**, (this will be done when the evidence is secured). This will enable the police to conduct their enquiries expediently and facilitate the speedier return of seized computer equipment to their owners.

The above information is not an exhaustive list and any other information noted on screen should be included.

Actions taken

Please give full details of other agencies that have been informed. If the police have not been informed, this must be noted, together with reasons, as e-safety incidents extend well beyond 'grooming' and may be linked to other criminal activity. This may include racist incidents, radicalisation or bullying online, please see legal framework section 4.2 for a comprehensive list. The form must then be signed and dated and handed as soon as possible to the person responsible for child protection within your organisation

Burstwick Primary School

e-Incident Log Sheet 2 – "Notifications and Actions" – person with responsibility for child protection

To be completed by the person with responsibility for Safeguarding within the organisation		
Notifications:	Yes	No
1. Was notification to the Local Authority Designated Officer required? 2. If yes, what was the outcome? 3. Have you notified the police? 4. Please give details with **reference to guidance overleaf**. **NB This is not an exhaustive list there may be other actions you are required to carry out within your specific organisation.**		

Conclusion to the incident:

Have specific vulnerabilities or trends been identified?	Yes	No

If yes, what action will now be taken?

Name of person completing this form:			
Organisation:			

Notifications

Please give full details of other agencies that have been informed. The person initially identifying the incident may have already contacted others, please also record them here, plus any additional action taken by you after receiving the completed Log Sheet 1.

As with Log Sheet 1, if the police have not been informed, this must be noted, together with reasons, as safety incidents extend well beyond 'grooming' and may be linked to other criminal activity. This may include racist incidents, radicalisation or bullying online, please see legal framework section 4.2 for a comprehensive list.

It is possible that information has not been recorded and secured by the member of staff completing Log Sheet 1. You are reminded that you have powers to detain and secure if you have reasonable grounds to believe that an offence IS being committed.

You may **detain the person (offender only)** and **secure any evidence** of the offence (including property). This would include the property of a victim or offender.
Once evidence is secured the Police may then seize the property under the Police & Criminal Evidence Act 1984.

Offences committed via computers/laptops/mobile phones.
In these situations the securing of information **must be carried out in a specific way** in order to obtain the best evidence possible for the police and other law enforcement agencies.
When a computer is turned on or on standby it should be **left exactly as it is**; in order to allow a trained seizure officer to attend. In all cases; attempts should be made to **record in note form** any details that can be seen on the screen. **DO NOT follow any links or change any pages**.
Information that should be noted if on screen:
o Website address.
o Email addresses of sender and recipient.
o Dates and Times.
o User names.
o Mobile phone numbers.
o Any profile information
o Any text from chat conversations.
If a request for inappropriate behaviour is made on MSN, FACEBOOK, any chat forum or Social networking site. **DO NOT DELETE or interfere with the offending account**, (this will be done when the evidence is secured). This will enable the police to conduct their enquiries expediently and facilitate the speedier return of seized computer equipment to their owners. The above information is not an exhaustive list and any other information noted on screen should be included.

Conclusion to the incident

Please record any disciplinary action taken or communications with parents or carers, as well as specific detail of future meetings, monitoring or discussion planned.

Vulnerabilities and Trends

If there are additional vulnerabilities and trends that have been revealed by the incident, there may be a need to review organisational policy or pass information to other agencies at a later date, either once the investigation has been concluded or even before that. Please record all details that you are able to provide at this stage.