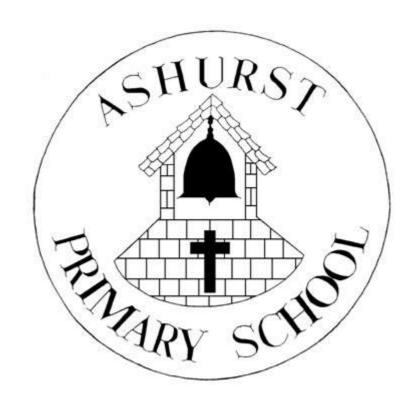
ASHURST CE AIDED PRIMARY SCHOOL



COVID-19 School Closure arrangements

Safeguarding and Child Protection Policy Annex

Based on WSCC Model Policy

JANUARY 2021

ASHURST CE AIDED PRIMARY SCHOOL

COVID-19 school closure arrangements for Safeguarding and Child Protection Policy Annex

JANUARY 2021

School Name: ASHURST CE AIDED PRIMARY SCHOOL Policy owner: Ashurst CE Aided Primary School Governors

Date adopted: 27th January 2021

Date shared with staff: 27th January 2021

This policy is for use during the COVID-19 school closure from 5th January 2021 only

1.Context

From 5th January 2021 government guidance requires all schools to partially close for the period of interim COVID-19 arrangements.

On 7th January 2021 The Department for Education issued 'Restricting attendance during the national lockdown: schools. Guidance for all schools in England'.¹

Page 39 of that guidance indicates that schools and colleges should review their child protection policies to reflect the move to remote education for pupils who are not attending school.

This annex does not cover all the other areas in the 'Restricted Attendance guidance' for example, parents and carers who are critical workers, wearing of face coverings, or good respiratory hygiene. Schools and colleges should review the guidance and ensure it is adapted to suit the needs of their particular setting.

This annex is supplementary guidance for the period of lockdown '3', from January 2021 only. During this period All schools and colleges MUST CONTINUE to have regard for the statutory guidance Keeping Children Safe in Education 2020²

 $\frac{https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment \ data/file/950510/School \ national \ restrictions \ guidance.pdf}$

¹

² https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

2. COVID19 from January 2021 annex for your current child protection policy.

This annex of the Ashurst CE Aided Primary School Safeguarding, and Child Protection policy will take effect from January 5th 2021 and remain in place during this period of time and will be reviewed as government policy and guidance changes.

Contents

1. Context	
2. COVID19 from January 2021 annex for your current child protection policy	
3. Key contacts	
3. Staff Resilience – School Safeguarding Team	4
4. Capacity of DSL team in our school	
5. Safeguarding Training and Induction	6
5.1 DSL Training	6
5.2 Continual Professional Development	6
5.3 The DSL training dates for our staff are:	6
5.4 Staff training	6
5.5 Raising a Safeguarding Concern	
6. Vulnerable children	7
6.1 Identifying our Vulnerable Children	8
6.2 Identifying Our Vulnerable Children	8
6.3 Supporting Our Vulnerable Children who are attending school	8
6.4 Hearing the Voice of the Child	8
6.5 Vulnerable Children Not Attending	8
6.6 Leave of Absence	8
7. Special schools and specialist post 16 provision	g
8. Boarding and residential schools, including international pupils	9
8.2 Private Fostering	10
9. Recruitment, Supply and other temporary staff or peripatetic teachers	10
9.1 Lateral Flow or other testing – volunteers.	10
10. Remote Education	10
11. Delivering Remote Education Safely and Safeguarding	10
12. Pupil wellbeing and Support	10
13. Support from the Local Authority	11
Appendix A – Identifying Vulnerable Children – suggested template	12
Appendix B - Delivering Remote Education Safely and Safeguarding	13
Appendix C – Children Requiring Mental Health Support	4 4
Self-Harm Guidance for Schools	45

3. Key contacts

Role	Name	Contact	Email
		number	
Designated Safeguarding Lead	Mrs S Smith		head@ashurstcofe-pri.w-sussex.sch.uk DSL@ashurstcofe-pri.w-sussex.sch.uk
Main Contact			
Designated Safeguarding Lead	Mrs T Clarke		head@ashurstcofe-pri.w-sussex.sch.uk DSL@ashurstcofe-pri.w-sussex.sch.uk
Designated Safeguarding Lead	Mrs A Hedley		MHedley2@ashurstcofe-pri.w-sussex.sch.uk DSL@ashurstcofe-pri.w-sussex.sch.uk
Co Headteachers	Mrs T Clarke & Mrs S Smith	01403 710426	head@ashurstcofe-pri.w-sussex.sch.uk
Chair of Governors	Mr R Allan	07971281785	RAllan@ashurstcofe-pri.w-sussex.sch.uk
MASH WSCC		(Out of Hours – 0330 222 6664)	Referrals to MASH should be made on the following web-based forms which can be accessed here: Adults - https://www.westsussex.gov.uk/raiseaconcernaboutanadult Children's - www.westsussex.gov.uk/Raiseaconcernaboutachild Referrals can also be made by telephone to 01403 229900
	Donna Tomlinson		LADO@westsussex.gov.uk
Safeguarding in Education		0330 222 4030	safeguarding.education@westsussex.gov.uk

3. Staff Resilience – School Safeguarding Team

It is expected that our school will have a trained DSL (or deputy) available on site. However, it is recognised that on occasions there may be operational challenges to this. In such cases, for our school there are two options to consider:

- a trained DSL (or deputy) from the school can be available to be contacted via phone or online video, for example working from home
- sharing trained DSLs (or deputies) with other schools (who should be available to be contacted via phone or online video)

Should we not have a DSL available on the telephone nor from another school, the member of staff operationally in charge of the school at that time will be responsible for co-ordinating safeguarding on site.

If we are aware we may face the possibility of not having a DSL available either on the school site, on the telephone, or from another school we will make immediate contact with the WSCC Safeguarding in Education Team on 0330 222 4030 or email safeguarding.education@westsussex.gov.uk for advice and support.

4. Capacity of DSL team in our school

There are currently three trained DSL's at Ashurst CE Aided Primary providing coverage. Contingency planning is that at all times there is at least one DSL on the school site. All DSL's are available at other times by telephone or email.

The Designated Safeguarding Lead is: Mrs Sarah Smith Trained DSL's also available: Mrs T Clarke & Mrs A Hedley

Contact Details:

Role	Name	Contact	Email
Lead DSL	Mrs S Smith	01403 710426	DSL@ashurstcofe-pri.w-sussex.sch.uk SSmith2@ashurstcofe-
			pri.w-sussex.sch.uk
DSL	Mrs T Clarke	01403 710426	DSL@ashurstcofe-pri.w-sussex.sch.uk
			TClarke2@ashurstcofe- pri.w-sussex.sch.uk
DSL	Mrs A Hedley	01403 710426	DSL@ashurstcofe-pri.w-sussex.sch.uk
			MHedley2@ashurstcofe- pri.w-sussex.sch.uk

All regular duties of the Safeguarding and Child Protection team in our school will remain during this period of lockdown in order to protect all of children and young people, whether they are attending school or accessing learning remotely.

This will include:

- Managing concerns raised
- Updating and managing access to safeguarding and child protection records by liaising with the offsite DSL (or deputy)
- Undertaking risk assessments for all pupils as necessary
 Co-ordinating safeguarding provision and checks for all vulnerable pupils on and off site

• Liaising with children's social workers where they require access to children to carry out statutory assessments at the school or college and engaging with key safeguarding partners when requested, in an appropriate and safe manner.

5. Safeguarding Training and Induction

Keeping Children Safe in Education 2020 states:

72. The designated safeguarding lead and any deputies should undergo training to provide them with the knowledge and skills required to carry out the role. The training should be updated every two years.

73. In addition to their formal training as set out above, their knowledge and skills should be updated (for example via e-bulletins, meeting other designated safeguarding leads, or taking time to read and digest safeguarding developments), at regular intervals, and at least annually, to keep up with any developments relevant to their role.

5.1 DSL Training

Our school recognises both DSL induction and refresher courses have been made available by WSCC as on-line courses and which can only be booked via the Safeguarding in Education pages on the West Sussex Service for Schools Site. We will ensure all our DSLs are trained within their two-year cycle.³

Our school will also consider if we need to train additional DSLs to mitigate the risk of the majority of our DSL team being away from work and not contactable.

5.2 Continual Professional Development

We also recognise the Safeguarding in Education pages on West Sussex Service for Schools contain many resources for DSL continual professional development, including a digital library and other relevant information.

5.3 The DSL training dates for our staff are:

Name of staff member	Type of training and date of issue	Role in school	
Mrs S Smith	DSL Refresher October 2019	Lead DSL	
Mrs T Clarke	DSL Refresher November 2019	DSL	
Mrs A Hedley	DSL Refresher January 2020	DSL	

5.4 Staff training

³ https://schools.westsussex.gov.uk/

All existing school staff have had safeguarding training and have read part 1 of Keeping Children Safe in Education (2020). All staff are aware of WSCC procedures for referral and have access to key contacts to do this.

Any new staff, including volunteers, who join the school will receive full safeguarding training.

5.5 Raising a Safeguarding Concern

All staff will continue to follow the normal processes as outlined in our child protection and safeguarding policy for raising safeguarding concerns about any child or young person, whether they attend our school or receive education elsewhere.

6. Vulnerable children

The Department for Education have identified vulnerable children as those who4:

- 1. are assessed as being in need under section 17 of the Children Act 1989, including children and young people who have a Child In Need plan, a Child Protection plan or who are a looked-after child
- 2. have an education, health and care (EHC) plan
- 3. have been identified as otherwise vulnerable by educational providers or local authorities (including children's social care services), and who could therefore benefit from continued full-time attendance, this might include:
- children and young people on the edge of receiving support from children's social care services or in the process of being referred to children's services
- adopted children or children on a special guardianship order
- those at risk of becoming NEET (not in employment, education or training)
- those living in temporary accommodation
- those who are young carers
- those who may have difficulty engaging with remote education at home (for example due to a lack of devices or quiet space to study)
- care leavers
- others at the provider and local authority's discretion including pupils and students who need to attend to receive support or manage risks to their mental health

⁴ https://www.gov.uk/government/publications/coronavirus-covid-19-maintaining-educational-provision/guidance-for-schools-colleges-and-local-authorities-on-maintaining-educational-provision#vulnerable-children-and-young-people

6.1 Identifying our Vulnerable Children

Our school will use the above definitions to identify our vulnerable children. We will generate a confidential system, accessed only by those who need to know, so we can identify each vulnerable child and monitor attendance and other concerns.

We recognise in the DfE guidance that all schools and colleges are expected to allow and strongly encourage vulnerable children and young people to attend and that parents/carers of vulnerable children and young people are strongly encouraged to take up the place.

Our school college will support this using DfE & LA Guidance and the school's Admissions policy

6.2 Identifying Our Vulnerable Children

Appendix A below is a suggested way in which you can identify your vulnerable children and a means to monitor attendance and / or contact with the child and families.

6.3 Supporting Our Vulnerable Children who are attending school

We will continue with our normal processes of supporting our vulnerable children when they are at school. This will include using such tools as 'Day in My Life' as necessary.

6.4 Hearing the Voice of the Child

Our school is very aware that the usual members of staff, whom children and young people may go to when needing to share their worries, may not be physically present at school or immediately available due to self-isolating etc. We will ensure all of our children and young people know who they can go to should they have worries if their usual staff member is unavailable.

6.5 Vulnerable Children Not Attending

If any of our vulnerable children and young people do not attend, our school / college will:

- work together with the local authority and social worker (where applicable) to follow up with the parent
 or carer to explore the reason for absence, discussing their concerns using supporting guidance
 considering the child's circumstances and their best interests
- work together with the local authority and social worker (where applicable) and other relevant partners to encourage the child or young person to attend educational provision, particularly where the social worker agrees that the child or young person's attendance would be appropriate
- Maximise the opportunities to understand the lived experience of all of our children who are not attending during lockdown, and particularly those who we recognise are vulnerable.

6.6 Leave of Absence

Latest guidance states vulnerable children are still expected to attend school full time, they should not be marked as Code X if they are not in school (except if they are shielding, self-isolating or quarantining). If the parent of a vulnerable child wishes their child to be absent, the parent should let the school know.

The Department of Education expects schools to grant applications for leave of absence given the exceptional circumstances. This should be recorded as code C (leave of absence authorised by the school) unless another authorised absence code is more applicable.

Where our school / college grants a leave of absence to a vulnerable child or young person we will still speak to parents and carers, and social workers (where applicable) to explore the reasons for this and any concerns raised. The discussions should focus on the welfare of the child or young person and ensuring that the child or young person is able to access appropriate education and support while they are at home.

Where providers have had to temporarily stop on-site provision on public health advice, they should inform the local authority to discuss alternative arrangements for vulnerable children and young people and work towards welcoming back pupils as soon as possible, where feasible to do so.

Our school / college will work collaboratively with other schools and education providers and other local partners (including the local authority, social workers, police, youth services, key workers etc.) to maximise opportunities for face-to-face provision for vulnerable children.

Our school / college will continually review the safeguarding risks to our vulnerable children and young people and will raise concerns with Early Help and / or MASH when and where relevant.

7. Special schools and specialist post 16 provision

Latest guidance indicates the Department of Education position of wanting children and young people in special schools, including residential special schools, and special post-16 institutions to continue to receive high-quality teaching and specialist professional support. This is because we know that children and young people with special educational needs and disabilities (SEND), and their families, can be disproportionately impacted by being out of education.

Special schools should continue to welcome and encourage pupils to attend full-time where the parent/carer wishes for their child to be able to attend. Special post-16 settings should continue to welcome and encourage students to attend as per their usual timetable where the young person wishes to attend.

On occasion special schools may encounter circumstances where they cannot provide their usual interventions and provision at adequate staffing ratios, or with staff with vital specialist training.

In these circumstances our school will seek to resume as close as possible to the child of young person's specified provision as soon as possible.

We also recognise pupil level risk assessments, which were used last spring, should not be used to filter children and young people in or out of attendance, but could be helpful to prioritise the provision a child or young person can get if full time provision for all is not possible.

8. Boarding and residential schools, including international pupils

Vulnerable children and the children of critical workers who have already travelled to their boarding school should continue to receive face to face education. Where other pupils have already travelled to their boarding school, in anticipation of school starting, they can continue to receive remote education in their boarding houses.

Vulnerable children and the children of critical workers who have not yet done so can return to their boarding school to receive face to face education. Where other pupils have not yet returned to their boarding school, they should not travel and should receive remote education at home

8.2 Private Fostering

We recognise that if any of our students are accommodated with a host family for 28 days or more then we will share the information with WSCC MASH (contact details above) to enable private fostering assessments to be undertaken.

9. Recruitment, Supply and other temporary staff or peripatetic teachers

Our school will follow our normal procedures for safer recruitment and will continue to undertake all necessary safeguarding and right to work checks for any new members of staff, supply cover or other temporary staff, including volunteers, who come into our school or college.

9.1 Lateral Flow or other testing – volunteers

We will ensure that any volunteers who attend our school to assist with lateral flow testing, or any other testing, will be subject to the same safer-recruiting checks as any other volunteer. If that is not possible in the time frames available to complete all of those checks then those volunteers will be supervised by school staff, who do have the relevant checks in place, at all times.

10. Remote Education

Our school recognises the temporary continuity direction⁵ which makes it clear that schools and colleges have a duty to provide remote education for state-funded, school-age children whose attendance would be contrary to government guidance or law around coronavirus (COVID-19).

Remote Education will be provided in accordance with DfE guidelines and for Ashurst CE Aided Primary School will be based on the Google G-Suite for Education platform, with supporting platforms such as Purple Mash as required. E-Safety and safeguarding will be paramount throughout.

11. Delivering Remote Education Safely and Safeguarding

Appendix B of this Annex outlines how our school and college will deliver remote education safely.

12. Pupil wellbeing and Support

Our school / college recognise that our children and young people may be experiencing a variety of emotions in response to the coronavirus (COVID-19) outbreak, such as anxiety, stress or low mood. This may particularly be the case for vulnerable children, including those with a social worker and young carers. It is important to contextualise these feelings as normal responses to an abnormal situation. Some may need support to re-adjust, either to a return to learning at home or being in school without their peers, and some may be showing signs of more severe anxiety or depression. Others will not be experiencing any challenges and will be content with the change in circumstances.

The return to remote learning for most will limit pupils' social interaction with their peers, carers and teachers, which may have an impact on wellbeing.

⁵ https://www.gov.uk/government/publications/remote-education-temporary-continuity-direction-explanatory-note

In order to support our pupils' wellbeing, we will work with our children, families and partner agencies to support our children and young people.

Please see Appendix C for further information.

13. Support from the Local Authority

The WSCC Safeguarding in Education Team are offering daily safeguarding support to schools and can be contacted by:

Phone - 0330 222 4030

Email - safeguarding.education@westsussex.gov.uk

Appendix A — Identifying Vulnerable Children — suggested template

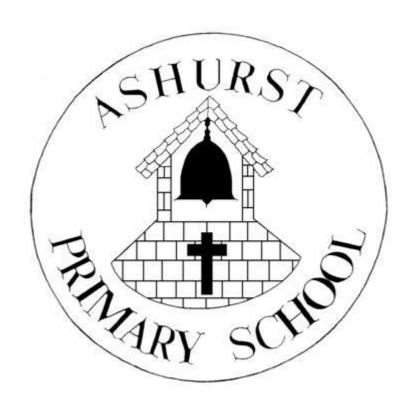
			Monitoring Our Vulr	nerable Children	
Name	Reason for Vulnerable	Place accepted Y/N?	Reasons provided by parent / carer if Not attending	If not attending – engagement plan	Log of concerns and contact details added to safeguarding file and date added.
A	Emerging concerns around mental health	Y			
В	Child in Need Plan	N	Mum states she can manage the child at home. Mum is furloughed and can support learning.	 Weekly contact by DSL and social worker to monitor and identify any escalations in risk. Monitor learning with at least weekly contact by class teacher. 	
С	Child cannot access remote learning	N	Mum states they are asking family for a tablet or laptop.	School are sending learning home. School will monitor and discuss progress with mum. School are also trying to resource a laptop.	

Appendix B - Delivering Remote Education Safely and Safeguarding



ASHURST CE AIDED PRIMARY SCHOOL





E-SAFETY POLICY

SEPTEMBER 2019

Revised January 2020 & Reviewed March 2020 due to Covid-19 pandemic

CONTENTS

	Introduction	Page 2			
1.	Key Responsibilities for the Community	Page 3			
	1.1 School management and leadership team	_			
	1.2 Designated Safeguarding Lead				
	1.3 All members of staff				
	1.4 Staff managing the technical environment				
	1.5 Children and young people				
	1.6 Parents and carers				
2.	Online Communication and Safer Use of Technology	Page 5			
	2.1 Managing the school website	_			
	2.2 Publishing videos and images online				
	2.3 Managing email				
	2.4 Official videoconferencing and webcam use for educational purposes				
	2.5 Appropriate and safe classroom use of the internet and any associated devices				
	2.6 Management of school learning platforms				
3.	Social Media Policy				
	3.1 General social media use				
	3.2 Official social media use				
	3.3 Staff personal use				
	3.4 Staff official use				
	3.5 Pupils use				
4.	Use of Personal Devices and Mobile Phones	Page 12			
	4.1 Rationale				
	4.2 Expectations for safe use				
	4.3 Pupils use				
	4.4 Staff use				
	4.5 Visitors use				
5.	Policy Decisions	Page 14			
	5.1 Reducing online risks				
	5.2 Internet use throughout the wider school community				
	5.3 Authorising internet access				
6.	Engagement Approaches	Page 15			
	6.1 Engagement and education of children and young people				
	6.2 Engagement and education of children and young people considered to be vulnerable				
	6.3 Engagement and education of staff				
	6.4 Engagement and education of parents and carers				
7.	Managing Information Systems	Page 16			
	7.1 Personal data online				
	7.2 Security and management				
	7.3 Password policy				
	7.4 Filtering and monitoring				
	7.5 Management of applications (apps) used to record children's progress				
8.	Responding to Online Incidents and Safeguarding Concerns	Page 18			

Page 19

- 9.1 Youth Produced Sexual Imagery (YPSI) or 'Sexting'
- 9.2 Online Child Sexual Abuse and Exploitation (CSAE)
- 9.3 Indecent Images of Children (IIOC)
- 9.4 Radicalisation and extremism
- 9.5 Cyberbullying

INTRODUCTION

Ashurst CE Aided Primary School (APS) believes that online safety is an essential element of safeguarding children and adults in the digital world when using technology such as computers, tablets, mobile phones or games consoles.

Internet and information communication technologies (ICT) are an important part of everyday life, therefore children must be supported to be able to learn how to develop strategies to manage and respond to risk, and be empowered to build resilience online. Ashurst Primary School has a duty to provide the school community with quality internet access in order to raise education standards, promote achievement, support professional work of staff and enhance management functions, and identifies that there is a clear duty to ensure that all pupils and staff are protected from potential harm online where possible.

The purpose of Ashurst Primary School's E-Safety Policy is to:

- Clearly identify the key principles expected of all members of the community with regards to the safe and responsible use of technology, thus ensuring that Ashurst Primary School is a safe and secure environment
- Safeguard and protect all members of Ashurst Primary School community online
- Raise awareness with all members of the Ashurst Primary School community, regarding the
 potential risks as well as benefits of technology
- Enable staff to work safely and responsibly, to role model positive behaviour online and be aware of the need to manage their own standards and practice when using technology
- Identify clear procedures to use when responding to online safety concerns that are known by all members of the community.

This policy applies to all staff including the governing body, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for or provide services on behalf of the school (collectively referred to as 'staff' in this policy), as well as pupils and parents/carers.

This policy applies to all access to the internet and use of information communication devices, including personal devices, or where pupils, staff or other individuals have been provided with school issued devices for use off-site, such as a work laptops, tablets or mobile phones.

This policy must be read in conjunction with other relevant school policies including (but not limited to) Safeguarding and Child Protection, Anti-bullying, Behaviour, Data Security (GDPR), Use of Images, Acceptable Use Policies (AUPs), Social Media, Confidentiality, as well as relevant curriculum policies including Computing, Personal Social and Health Education (PSHE), Relationships and Sex Education (RSE).

1. Key Responsibilities

1.1 Key responsibilities of the school management and leadership team are:

- To develop, own and promote the online safety vision and culture to all stakeholders, in line with national and local recommendations with appropriate support and consultation throughout the school community
- To ensure that online safety is viewed by the whole community as a safeguarding issue and proactively developing a robust online safety culture
- To support the Designated Safeguarding Leads (DSL) by ensuring they have sufficient time and resources to fulfil their online safety role and responsibilities.
- To ensure there are appropriate and up-to-date policies and procedures regarding online safety, including an Acceptable Use Policy (AUP) which cover appropriate professional conduct and use of technology
- To ensure that suitable and appropriate filtering and monitoring systems are in place to protect children from inappropriate content which meet the needs of the school community whilst ensuring children have access to required educational material
- To work with and support technical staff in monitoring the safety and security of school systems and networks, and to ensure that the school network system is actively monitored
- To ensure all members of staff receive regular, up-to-date and appropriate training regarding online safety roles and responsibilities, and provide guidance regarding safe appropriate communications
- To ensure that online safety is embedded within a progressive whole school curriculum which enables all pupils to develop an age-appropriate understanding of online safety and the associated risks and safe behaviours
- To be aware of any online safety incidents and ensure that external agencies and support are liaised with, as appropriate

- To receive and regularly review online safeguarding records and use them to inform and shape future practice
- To ensure there are robust reporting channels for the school community to access regarding online safety concerns, including internal, local and national support
- To ensure that appropriate risk assessments are undertaken regarding the safe use of technology, including ensuring the safe and responsible use of devices
- To ensure a member/members of the Governing Body are identified with a lead responsibility for supporting online safety
- To audit and evaluate current online safety practice to identify strengths and areas for improvement
- To ensure that the Designated Safeguarding Leads (DSLs) are aware of current polices and procedures and are kept up to date with current practise.

1.2 Key responsibilities of the Designated Safeguarding Lead is:

- To act as a named point of contact on all online safeguarding issues and liaise with other members of staff and other agencies, as appropriate
- To keep up-to-date with current research, legislation and trends regarding online safety
- To coordinate participation in local and national events to promote positive online behaviour where appropriate
- To ensure that online safety is promoted to parents and carers and the wider community through a variety of channels and approaches
- To work with the school lead for data protection and data security to ensure that practice is in line with current legislation
- To maintain a record of online safety concerns/incidents and actions taken as part of the schools safeguarding recording structures and mechanisms
- To monitor the school's online safety incidents to identify gaps/trends and use this data to update the school education response to reflect need
- To report to the school management team, Governing Body and other agencies, as appropriate, on online safety concerns and local data/figures
- To liaise with the local authority and other local and national bodies, as appropriate
- To work with the school leadership and management to review and update the online safety policies, Acceptable Use Policies (AUPs) and other related policies on a regular basis (at least annually) with stakeholder input
- To ensure that online safety is integrated with other appropriate school policies and procedures.

1.3 Key responsibilities for staff members are:

- To contribute to the development of online safety policies
- To read the school Acceptable Use Policies (AUPs) and adhere to them
- To take responsibility for maintaining the security of school systems and data
- To have an awareness of a range of different online safety issues and how they may relate to the pupils in their care
- To model good practice when using new and emerging technologies
- To embed online safety education in curriculum delivery wherever possible
- To identify individuals of concern and take appropriate action by following school safeguarding policies and procedures
- To know when and how to escalate online safety issues, internally and externally
- To be able to signpost to appropriate support available for online safety issues, internally and externally
- To maintain a professional level of conduct in their personal use of technology, both on and off site.

1.4 Key responsibilities for staff managing the technical environment are:

- To provide a safe and secure technical infrastructure which supports safe online practices,
 whilst ensuring that learning opportunities are still maximised
- To take responsibility for the implementation of safe security of systems and data in partnership with the leadership and management team
- To ensure that suitable access controls and encryption is implemented to protect personal and sensitive information held on school-owned devices
- To ensure that the school's filtering policy is applied and updated on a regular basis, and that responsibility for its implementation is shared with the DSL
- To ensure that the use of the school's network is regularly monitored and report any deliberate or accidental misuse to the DSL
- To report any breaches or concerns to the DSL and Leadership Team, and together ensure that they are recorded and appropriate action is taken, as advised
- To develop an understanding of the relevant legislation, as it relates to the security and safety of the technical infrastructure
- To report any breaches and liaise with the local authority (or other local or national bodies), as appropriate, on technical infrastructure issues
- To provide technical support and perspective to the DSL and Leadership Team, especially in the development and implementation of appropriate online safety policies and procedures
- To ensure that the school's ICT infrastructure/system is secure and not open to misuse or malicious attack
- To ensure that appropriate anti-virus software and system updates are installed and maintained on all setting machines and portable devices.

1.5 Key responsibilities of pupils are:

- To contribute to the development of online safety policies
- To read and sign the pupil Acceptable Use Policy (AUP) and adhere to them
- To respect the feelings and rights of others, both on and offline
- To seek help from a trusted adult if anything causes concern, and support others that may be experiencing online safety issues.

At a level that is appropriate to their individual age, ability and vulnerabilities:

- To take responsibility for keeping themselves and others safe online
- To take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies
- To assess the personal risks of using any particular technology, and behave safely and responsibly to limit those risks.

1.6 Key responsibilities of parents and carers are:

- To read the school Acceptable Use Policies, encouraging their children to adhere to them, and adhering to the policies themselves, where appropriate
- To discuss online safety issues with their children, supporting the school in their online safety approaches, and reinforcing appropriate safe online behaviours at home
- To be a role model for the safe and appropriate uses of technology and social media
- To identify changes in behaviour that could indicate that their child is at risk of harm online
- To seek help and support from the school, or other appropriate agencies, if they or their child encounter online problems or concerns
- To contribute to the development of the school online safety policies
- To use school systems, such as learning platforms and other network resources, safely and appropriately
- To take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.

2. Online Communication and Safer Use of Technology

2.1 Managing the school website:

- Ashurst CE Primary School seeks to ensure that information posted on the school website meets the requirements as identified by the Department for Education (DfE).
- The contact details on the website will be the school address, email and telephone number. Staff and/or pupils' personal information will not be published.
- The Headteacher and E-Learning Manger will ensure that information uploaded to the school website is both accurate and appropriate.
- The website will comply with the school's guidelines for publications, including accessibility and respect for intellectual property rights, privacy policies and copyright.
- Pupils work will be published with their permission or that of their parents/carers.
- Security procedures will ensure that the administration of the school website is only undertaken by designated staff as appropriate, and access secured with an appropriately strong password.
- Ashurst Primary School will seek to post appropriate information about safeguarding, including online safety, on the school website for members of the community.

2.2 Publishing images and videos online:

- Ashurst CE Primary School will ensure that all images and videos shared online are used in accordance with the school's Use of Images Policy.
- Ashurst CE Primary School will ensure that all use of images and videos take place in accordance with other policies and procedures, including Data Security, Acceptable Use Policies, Codes of Conduct, social media, use of personal devices and mobile phones etc.
- In line with the Use of Images Policy, written permission from parents or carers will always be obtained before images/videos of pupils are electronically published.

2.3 Managing email:

- All members of staff are provided with a specific school email address to use for any
 official communication.
- The use of personal email addresses by staff for any official school business is not permitted unless exceptional circumstances are identified and approved e.g loss of school communication systems.
- The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains any content which could be subject to data
 protection legislation (e.g. sensitive or personal information) will only be sent using secure
 and encrypted email.
- Access to school email systems will always take place in accordance to data protection legislation and in line with other appropriate school policies e.g. Confidentiality.

- Members of the community must immediately tell a designated member of staff if they
 receive offensive communication and this will be recorded in the school safeguarding
 files/records.
- Staff will be encouraged to develop an appropriate work life balance when responding to work related email. School Policy at present is that all electronic communication from parents for staff comes via School Office in the first instance.
- Excessive social email use can interfere with teaching and learning and will be restricted.
- Emails sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be.
- School email addresses and other official contact details must not be used for setting up personal social media accounts.

2.4 Videoconferencing and webcam use for educational purposes:

- The school acknowledges that videoconferencing is a challenging activity with a wide range
 of learning benefits. Preparation and evaluation are essential to the whole activity.
- All videoconferencing equipment will be switched off when not in use and where appropriate, not set to auto answer.
- Staff will ensure that external videoconference opportunities and/or tools are suitably risk assessed and will ensure that accounts and systems used to access events are appropriately safe and secure.

Users:

- Pupils will ask permission from a teacher before making or answering a videoconference call or message.
- Videoconferencing will be supervised at all times by a teacher.
- Parents/carers consent will be obtained prior to children taking part in videoconferencing activities.
- Video conferencing will take place via official and approved communication channels following a robust risk assessment.

Content:

When recording a videoconference lesson, written permission will be given by all sites and
participants. The reason for the recording must be given and the recording of
videoconference should be clear to all parties at the start of the conference. Recorded
material will be stored securely.

- If third party materials are to be included, APS will check that recording is acceptable to avoid infringing the third-party intellectual property rights.
- APS will establish dialogue with other conference participants before taking part in a videoconference. If it is a non-school site, Ashurst Primary School will check that they are delivering material that is appropriate for the pupils.

2.5 Classroom use of the internet and any associated devices:

- Internet use is a key feature of educational access and all children will receive age and ability appropriate education to support and enable them to develop strategies to respond to concerns, as part of an embedded whole school curriculum. Please access specific curriculum policies for further information.
- The school's internet access will be designed to enhance and extend education.
- Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.
- All members of staff are aware that they cannot rely on filtering alone to safeguard children and supervision, classroom management and education about safe and responsible use is essential.
- ✓ Supervision of pupils will be appropriate to their age and ability:
 - At Early Years Foundation Stage and Key Stage 1, pupils' access to the internet will be by adult demonstration with occasional directly supervised access to specific and approved online materials which support the learning outcomes planned for the pupils' age and ability.
 - At Key Stage 2, pupils will be supervised. Pupils will use age-appropriate search engines and online tools, and online activities will be teacher-directed where necessary. Children will be directed to online material and resources which support the learning outcomes planned for the pupils' age and ability.
 - Where appropriate in residential provisions, Ashurst Primary School will balance pupils' ability to take part in age appropriate peer activities online with the need for the school to detect abuse, bullying or unsafe practice by children in accordance with the National Minimum Standards (NMS).
- All school owned devices will be used in accordance with the school Acceptable Use Policy and with appropriate safety and security measures in place.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- Pupils will be educated in the effective use of the internet in research, including the skills
 of knowledge location, retrieval and evaluation.

- The school will use age appropriate search tools where possible, e.g. Google Safe Search, CBBC safe search, Dorling Kindersley Find Out, Kiddle etc., as decided by the school following an informed risk assessment to identify which tool best suits the needs of our community.
- The school will ensure that the use of internet-derived materials by staff and pupils complies with copyright law and acknowledge the source of information.
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The evaluation of online materials is a part of teaching and learning in every subject, and will be viewed as a whole-school requirement across the curriculum.
- Ashurst CE Primary School will use the internet in order to enable pupils and staff to communicate and collaborate in a safe and secure environment.

2.6 Management of school learning platforms:

- Leaders and staff will regularly monitor the usage of the learning platform in all areas, in particular message and communication tools and publishing facilities.
- Pupils/staff will be advised about acceptable conduct and use when using the learning platform.
- Only members of the current pupil, parent/carers and staff community will have access to the learning platform.
- All users will be mindful of copyright issues and will only upload appropriate content onto the learning platform.
- When staff, pupils' etc. leave the school, their account or rights to specific school areas will be disabled or transferred to their new establishment where appropriate.
- Any concerns about content on the learning platform will be recorded and dealt with in the following ways:
 - a) The user will be asked to remove any material deemed to be inappropriate or offensive.
 - b) The material will be removed by the site administrator if the user does not comply.
 - c) Access to the learning platform for the user may be suspended.
 - d) The user will need to discuss the issues with a member of leadership before reinstatement.
 - e) A pupil's parent/carer may be informed.
- Visitors may be invited onto the learning platform by a member of the leadership team where appropriate. In this instance, there may be an agreed focus or a limited time slot allocated.

• Pupils may require editorial approval from a member of staff. This may be given to the pupil to fulfil a specific aim and may have a limited time frame.

3. Social Media Policy

3.1 General social media use:

- Expectations regarding safe and responsible use of social media will apply to all members of the Ashurst Primary School community and exist in order to safeguard both the school and the wider community, on and offline. Examples of social media may include blogs, wikis, social networking sites, forums, bulletin boards, multi-player online gaming, apps, video/photo sharing sites, chatrooms, instant messenger and many others.
- All members of the Ashurst Primary School community will be encouraged when engaging with social media in a positive, safe and responsible manner at all times.
- Information about safe and responsible use of social media will be communicated clearly and regularly to all members of the Ashurst Primary School community.
- All members of the APS community are advised not to publish specific and detailed private views, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
- APS will, in line with current policies, via filtering policies and procedures, restrict pupil
 and staff access to social media and social networking sites whilst on site and when using
 school provided devices and systems on the school network in order to protect the online
 environment within school.
- The use of social networking applications during school hours for personal use is not permitted, a school firewall is in place.
- Inappropriate or excessive use of social media during school hours or whilst using school devices may result in disciplinary or legal action and/or removal of internet facilities.
- Any concerns regarding the online conduct of any member of the APS community on social media sites should be reported to the Leadership Team and will be managed in accordance with policies such as Anti-bullying, Allegations Against Staff, Behaviour and Safeguarding/Child Protection.
- Any breaches of school policies may result in criminal, disciplinary or civil action being taken and this will depend upon the age of those involved and the circumstances of the wrong committed. Action taken will be in accordance with relevant policies, such as Antibullying, Allegations Against Staff, Behaviour and Safeguarding/Child Protection.

3.2 Official & school business use of Social media:

- Official use of social media sites by the school will only take place with clear educational or community engagement objectives with specific intended outcomes e.g. increasing parental engagement.
- Official use of social media sites as communication tools will be risk assessed and formally approved by the Headteacher & in discussion with the E-Learning manager.
- Official school social media channels where required will be set up as a distinct and dedicated social media site or account for educational or engagement purposes.
- Staff will use school provided email addresses to register for and manage any official approved social media channels.
- Members of staff running official social media channels will follow appropriate policy, e.g.
 Twitter policy, to ensure that they are aware of the required behaviours and expectations
 of use and to ensure that sites are used safely, responsibly and in accordance with local
 and national guidance and legislation.
- All communication on official social media platforms will be clear, transparent and open to scrutiny.
- Any online publication on official social media sites will comply with legal requirements, including the Data Protection Act 1998 right to privacy conferred by the Human Rights Act 1998, or similar duty to protect private information and will not breach any common law duty of confidentiality, copyright etc.
- Official social media use will be in line with existing policies, including Anti-bullying and Child Protection.
- Images or videos of children will only be shared on official social media sites/channels, in accordance with the 'Use of Images' policy.
- Information about safe and responsible use of social media channels will be communicated clearly and regularly to all members of the community.
- Official social media sites, blogs or wikis will be suitably protected (e.g. password protected) and where appropriate, run and/or linked to/from the school website and take place with written approval from the Leadership Team.
- Account information and relevant details for social media channels will be kept secure and
 in case of emergency, appropriate named staff only to have access (Awareness of possible
 staff absence will be catered for e.g Named alternative access available).
- Parents/carers and pupils will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.
- Public communications on behalf of the school will, where possible, be agreed by at least one other colleague.
- Official social media channels will link back to the APS website and/or Acceptable Use Policy to demonstrate that the account is official.
- The school will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

3.3 Staff personal use of social media:

- The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the school Acceptable Use Policy (AUP).
- All members of staff are advised not to communicate with or add as 'friends' any current
 or past children/pupils or current or past pupils' family members via any personal social
 media sites, applications or profiles. Any pre-existing relationships or exceptions that may
 compromise this will be discussed with the Designated Safeguarding Leads (DSL) and/or
 the Headteacher.
- If ongoing contact with pupils is required once they have left the school roll, then members of staff will be expected to use existing and official school provided communication tools.
- All communication between staff and members of the school community on school business will take place via official approved communication channels (such as an official school provided email address or phone numbers).
- Staff are advised to not use personal social media accounts to make contact with pupils or parents, nor should any contact be accepted, except in circumstances whereby prior approval has been given by the Headteacher.
- Any communication from pupils/parents received on personal social media accounts will be reported to the schools Designated Safeguarding Lead (DSL).
- Information and content that staff members have access to as part of their employment, including photos and personal information about pupils and their family members, colleagues etc. must not be shared or discussed on personal social media sites.
- All members of staff are strongly advised to safeguard themselves and their privacy when
 using social media sites. This will include being aware of location sharing services, setting
 the privacy levels of their personal sites as strictly as they can, opting out of public listings
 on social networking sites, logging out of accounts after use and keeping passwords safe
 and confidential.
- All members of staff are encouraged to carefully consider the information, including text
 and images, they share and post online, and to ensure that their social media use is
 compatible with their professional role, in accordance with school policies (Safeguarding,
 Confidentiality, Data Protection etc.) and the wider professional and legal framework.
- Members of staff will be encouraged to manage and control the content they share and
 post online. Advice will be provided to staff via staff training and by sharing appropriate
 guidance and resources on a regular basis.

- Members of staff will notify the Leadership Team immediately if they consider that any content shared or posted via any information and communications technology, including emails or social networking sites, conflicts with their role in the school.
- Members of staff are encouraged not to identify themselves as employees of Ashurst Primary School on their personal social networking accounts. This is to prevent information on these sites from being linked with the school and also to safeguard the privacy of staff members and the wider community.
- Members of staff will ensure that they do not represent their personal views as that of the school on social media.
- School email addresses will not be used for setting up personal social media accounts.

3.4 Staff official use of social media:

- If members of staff are participating in online activity as part of their capacity as an employee of the school, then they are requested to be professional at all times and to be aware that they are an ambassador for the school.
- Staff using social media officially will disclose their official role/position, but always make it clear that they do not necessarily speak on behalf of the school.
- Staff using social media officially will be responsible, credible, fair and honest at all times, and consider how the information being published could be perceived or shared.
- Staff using social media officially will always act within the legal frameworks they would adhere to within the workplace, including libel, defamation, confidentiality, copyright, data protection as well as equalities laws.
- Staff must ensure that any image posted on any official social media channel has appropriate written parental consent.
- Staff using social media officially will be accountable and must not disclose information, make commitments or engage in activities on behalf of the school unless they are authorised to do so.
- Staff using social media officially will inform their line manager, the Designated Safeguarding Leads and/or the Headteacher of any concerns, such as criticism or inappropriate content posted online.
- Staff will not engage with any direct or private messaging with children or parents/carers through social media and will only communicate via official communication channels.
- Staff using social media officially will follow the appropriate policy e.g Twitter, and have appropriate training and support in using this, as well as following professional responsibilities.

3.5 Pupils use of social media:

- Safe and responsible use of social media sites will be outlined for children and their parents as part of the Acceptable Use Policy.
- Personal publishing on social media sites will be taught to pupils as part of an embedded and progressive education approach via age appropriate sites which have been risk assessed and approved as suitable for educational purposes.
- Pupils will be advised to consider the risks of sharing personal details of any kind on social media sites which may identify them and/or their location. Examples would include real/full name, address, mobile or landline phone numbers, school attended, Instant Messenger contact details, email addresses, full names of friends/family, specific interests and clubs etc.
- Pupils will be advised not to meet any online friends without a parent/carer or other responsible adult's permission and only when they can be present.
- Pupils will be advised on appropriate security on social media sites and will be encouraged to use secure passwords, deny access to unknown individuals and be supported in learning how to block and report unwanted communications.
- Pupils will be encouraged to only approve and invite known friends on social networking sites
 and to deny access to others by making profiles private/protected.
- Parents will be informed of any official social media use with pupils and written parental consent will be obtained, as required.
- Any official social media activity involving pupils will be moderated by the school, where possible.
- The school is aware that many popular social media sites state that they are not for children under the age of 13, therefore Ashurst Primary School must not create accounts within school specifically for children under this age.
- Any concerns regarding pupils' use of social networking, social media and personal publishing sites, both at home and at school, will be dealt with in accordance with existing school policies, including Anti-bullying and Behaviour.
- Any concerns regarding pupils' use of social networking, social media and personal publishing sites, both at home and at school, will be raised with parents/carers, particularly when concerning any underage use of social media sites.

4. Use of Personal Devices and Mobile Phones

4.1 Rationale regarding personal devices and mobile phones:

 The widespread ownership of mobile phones and a range of other personal devices among children, young people and adults will require all members of the APS community to take steps to ensure that mobile phones and personal devices are used responsibly.

- The use of mobile phones and other personal devices by young people and adults will be decided by the school and is covered in appropriate policies including the school Acceptable Use Policy.
- Ashurst Primary School recognises that personal communication through mobile technologies is an accepted part of everyday life for pupils, staff and parents/carers, but requires that such technologies need to be used safely and appropriately within school.

4.2 Expectations for safe use of personal devices and mobile phones:

- All use of personal devices and mobile phones will take place in accordance with the law and other appropriate school policies.
- Electronic devices of all kinds that are brought in on site are the responsibility of the user at all times. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices, either potential or actual.
- Mobile phones and personal devices are not permitted to be used in certain areas within the school site. Mobile phones cannot be used within the classroom during school hours and should be stored in a safe place, unless pre-approved by the Headteacher and under exceptional circumstances.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community, and any breaches will be dealt with as part of the Discipline/Behaviour Policy.
- Members of staff will be issued with a work email address and will use the school landline phone when contact with pupils or parents/carers is required.
- All members of the Ashurst Primary School community will be advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene the school policies.
- School landline phones, mobile phones and devices must always be used in accordance with the Acceptable Use Policy.
- School mobile phones and devices used for communication with parents and pupils must be suitably protected via a passcode/password/pin and must only be accessed and used by members of staff.

4.3 Pupils use of personal devices and mobile phones:

- Pupils will be educated regarding the safe and appropriate use of personal devices and mobile phones.
- All use of mobile phones and personal devices by pupils will take place in accordance with the Acceptable Use Policy.

- Pupil's personal mobile phones and personal devices will be switched off and handed in to School Office in the morning to be kept securely throughout the school day. Pupils can collect mobile phones and personal devices from School Office at the end of the day.
- If a parent/carer needs to be contacted on behalf of a pupil, contact will be made via School Office using a school based phone.
- Parents are advised to contact the School Office direct at all times, not via the pupils own mobile phone.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members.
- Pupils will be instructed in safe and appropriate use of mobile phones and personal devices, and will be made aware of boundaries and consequences.
- Mobile phones and personal devices must not be taken into examinations. Pupils found in
 possession of a mobile phone or personal device during an exam will be reported to the
 appropriate examining body. This may result in the pupil's withdrawal from either that
 examination or all examinations.
- If a pupil breaches the school policy, then the phone or device will be confiscated and will be held in a secure place in School Office. Mobile phones and devices will be released to parents/carers in accordance with the school policy.
- If there is suspicion that material on a pupil's personal device or mobile phone may be illegal
 or may provide evidence relating to a criminal offence, then the device will be handed over
 to the police for further investigation.

4.4 Staff use of personal devices and mobile phones:

- Members of staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the school in a professional capacity. Any pre-existing relationships which could compromise this will be discussed with leaders.
- Staff will not use personal devices such as mobile phones, tablets or cameras to take photos or videos of children, and will only use work-provided equipment for this purpose.
- Staff will not use any personal devices directly with children and will only use workprovided equipment during lessons/educational activities.
- Members of staff will ensure that any use of personal phones and devices will always take
 place in accordance with the law e.g. data protection, as well as relevant school policies and
 procedures e.g. Confidentiality, Data Security, Acceptable Use etc.
- Staff personal mobile phones and devices will be switched off/switched to 'silent' and stored in staff cloakroom lockers/as appropriate away from the classrooms during school hours.
- Bluetooth or other forms of communication should be 'hidden' or switched off.

- Personal mobile phones or devices will not be used during teaching periods unless permission has been given by a member of the Leadership Team in emergency circumstances.
- Staff will ensure that any content bought on site via mobile phones and personal devices are compatible with their professional role and expectations.
- If a member of staff breaches the school policy then disciplinary action will be taken.
- If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence, then the police will be contacted.
- Any allegations against members of staff involving personal use of mobile phone or devices will be responded to following the school allegations management policy.

4.5 Visitors use of personal devices and mobile phones:

- Parents/carers and visitors must use mobile phones and personal devices in accordance with the school Acceptable Use Policy. Visitors must turn off their device and/or hand their device in to School Office, as appropriate, in accordance with school policies.
- Use of mobile phones or personal devices by visitors and parents/carers to take photos or videos must take place in accordance with the School Use of Images Policy.
- The school will ensure appropriate information is provided to inform visitors of expectations of use.
- Staff will be expected to challenge concerns when safe and appropriate, and will always inform the Designated Safeguarding Lead (DSL) of any breaches of use by visitors.

5. Policy Decisions

5.1 Reducing online risks:

- Ashurst CE Primary School is aware that the Internet is a constantly changing environment with new apps, tools, devices, sites and material emerging at a rapid pace.
- Emerging technologies will be examined for educational benefit and the school leadership team will ensure that appropriate risk assessments are carried out before use in school is allowed.
- The school will ensure that appropriate filtering and monitoring systems are in place to prevent staff and pupils from accessing unsuitable or illegal content. Entrust and Rivanet control and monitor filtering systems and solutions, including onsite.
- The school will take all reasonable precautions to ensure that users access only appropriate
 material. However, due to the global and connected nature of Internet content, it is not
 always possible to guarantee that access to unsuitable material will not occur via a school
 computer or device.
- The school will audit technology use to establish if the Online Safety policy is adequate and that the implementation of the policy is appropriate.

• Methods to identify, assess and minimise online risks will be reviewed regularly by the schools Leadership Team.

5.2 Internet use throughout the wider school community:

- The school will liaise with local organisations to establish a common approach to online safety.
- The school will work with the local community's needs (including recognising cultural backgrounds, languages, religions and ethnicity) to ensure internet use is appropriate.
- The school will provide an Acceptable Use Policy for any guest/visitor who needs to access the school computer system or Internet on site.

5.3 Authorising internet access:

- The school will maintain a current record of all staff and pupils who are granted access to the school's devices and systems.
- All staff, pupils and visitors will read and sign the Acceptable Use Policy before using any school resources.
- Parents will be informed that pupils will be provided with supervised internet access which is appropriate to their age and ability.
- Parents will be asked to read the Acceptable Use Policy for pupil access and discuss it with their child, where appropriate.
- When considering access for vulnerable members of the community (such as with pupils with special education needs), the school will make decisions based on the specific needs and understanding of the pupil(s).

6. Engagement Approaches

6.1 Engagement and education of children and young people:

- An Online Safety curriculum is established and embedded throughout the whole school, to raise awareness regarding the importance of safe and responsible internet use amongst pupils.
- Education about safe and responsible use will precede internet access.
- Pupils input will be sought when writing and developing school online safety policies and practices, including curriculum development and implementation e.g 'Pupils Voice'.
- Pupils will be supported in reading and understanding the Acceptable Use Policy in a way
 which suits their age and ability.

- All users will be informed that network and internet use will be monitored.
- Online safety will be included in the PSHE, RSE, Citizenship and Computing programmes of study, covering both safe school and home use.
- Online safety education and training will be included as part of the transition programme across the Key Stages and when moving between establishments.
- Safe and responsible use of the internet and technology will be reinforced across the curriculum and within all subject areas.
- External support will be used to complement and support the school's internal online safety education approaches where available. e.g NSPCC/PC Keeley.
- The school will implement peer education to develop online safety, as appropriate to the needs of the pupils.

6.2 Engagement and education of children and young people considered to be vulnerable:

- Ashurst Primary School is aware that some pupils may be considered to be more vulnerable online due to a range of factors.
- Ashurst Primary School will ensure that differentiated and ability appropriate online safety (e-Safety) education is given, with input from specialist staff as appropriate (e.g. SENCO, Looked after Child Coordinator).

6.3 Engagement and education of staff:

- The E-Safety policy will be formally provided to and discussed with all members of staff as part of induction, and will be reinforced and highlighted as part of our safeguarding responsibilities.
- Staff will be made aware that our internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential when using school systems and devices.
- Up-to-date and appropriate staff training in safe and responsible internet use, both professionally and personally, will be provided for all members of staff in a variety of ways, on a regular basis.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- Members of staff with a responsibility for managing filtering systems or monitoring of ICT use will have clear procedures for reporting issues or concerns.
- The school will highlight useful online tools which staff should use according to the age and ability of the pupils.

6.4 Engagement and education of parents and carers:

- Ashurst Primary School recognises that parents/carers have an essential role to play in enabling children to become safe and responsible users of the internet and digital technology.
- Parents' attention will be drawn to the school E-Safety policy and expectations in newsletters, letters, school prospectus and on the school website.
- A partnership approach to online safety at home and at school with parents will be
 encouraged. This may include offering parent evenings with demonstrations and
 suggestions for safe home internet use via information on the school's website, and/or
 highlighting online safety at other well attended events e.g. parent evenings, transition
 events, fetes and Sports Days.
- Parents will be requested to read, sign and return online safety information as part of the Home School Agreement.
- Parents will be encouraged to read the school Acceptable Use Policy for pupils and discuss its implications with their children.
- Information and guidance for parents on online safety will be made available to parents in a variety of formats, e.g. school website, emails home, social media as appropriate.
- Parents will be encouraged to role model positive behaviour for their children online.

7. Managing Information Systems

7.1 Managing personal data online:

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- Full information regarding the school's approach to data protection and information governance is available. e.g GDPR compliance

7.2 Security and management of information systems:

- The security of the school information systems and users access will be reviewed regularly.
- Virus protection will be updated regularly.
- Personal data sent over the internet or taken off site, e.g. via portable media storage, will be encrypted or accessed via appropriate secure remote access systems.
- Portable media may not be used without specific permission and the use of the school's anti-virus/malware scanning facilities on access.
- Unapproved software will not be allowed in work areas or attached to email.

- Files held on the school's network will be subject to appropriate checks e.g storage space, appropriateness of content & file size monitoring.
- The E-Learning Coordinator/Network Manager will review system capacity regularly.
- The appropriate use of user logins and passwords to access the school network will be enforced for all users.
- All users will be expected to log off or lock their screens/devices if systems are unattended.
- The school will log and record internet use on all school owned devices.

7.3 Password Policy

- All users will be informed not to share passwords or information with others, and not to login as another user at any time.
- Staff and pupils must always keep their passwords private and must not share it with others or leave it where others can find it.
- All members of staff will have their own unique username and passwords to access school systems. Members of staff are responsible for keeping their passwords private.
- Ashurst Primary School advises staff and pupils to use STRONG passwords for access into the school's network systems.
- Ashurst Primary School will advise staff to change their passwords on a regular basis.
- All pupils are provided with their own unique username and private passwords to access relevant accounts, e.g. TT Rockstars, Purple Mash etc, and/or picture passwords for their VLE accounts. Pupils are responsible for keeping their passwords private.

7.4 Filtering and Monitoring:

- The governors will ensure that the school has age and ability appropriate filtering and monitoring in place whilst using school devices and systems to limit pupils exposure to online risks.
- The school's internet access strategy will be dependent on the need and requirements of our community and will therefore be designed to suit the age and curriculum requirements of our pupils, with advice from technical, educational and safeguarding staff.
- All monitoring of school owned/provided systems will take place to safeguard members of the community.
- All users will be informed that use of school systems can be monitored and that all
 monitoring will be in line with data protection, human rights and privacy legislation.
- The school uses educational filtered secure broadband connectivity through Entrust, which
 is appropriate to the age and requirement of the school's pupils.

- The school uses the 'Webscreen' filtering system provided by Entrust, which blocks sites that fall into categories such as pornography, racial hatred, extremism, gaming, sites of an illegal nature, etc.
- The school adheres to WSCC procedures regarding broadband/filtering provider to ensure that filtering policy is continually reviewed.
- The school will have a clear procedure for reporting breaches of filtering which all members of the school community (all staff and pupils) will be made aware of.
- If staff or pupils discover unsuitable sites, the URL will be reported to the school E-Learning Manager/Designated Safeguarding Lead (DSL) and will then be recorded and escalated as appropriate.
- The school filtering system will block all sites on the Internet Watch Foundation (IWF) list.
- Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes, and where appropriate with consent from the Leadership Team.
- All changes to the school filtering policy will be logged and recorded.
- The Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective and appropriate.
- Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, Sussex Police or CEOP immediately.

7.5 Management of applications (apps) used to record children's progress:

- The school leadership team are responsible for the security of any data or images held of children.
- Apps/systems which store personal data will be risk assessed prior to use.
- Only school issued devices will be used for apps that record and store children's personal
 details, attainment or photographs. Personal staff mobile phones or devices will not be
 used to access or upload content to any apps which record and store children's personal
 details, attainment or images.
- Devices will be appropriately encrypted if taken off site to prevent a data security breach in the event of loss or theft.
- Users will be advised on safety measures to protect all members of the community, such as using strong passwords, logging out of systems etc.
- Parents will be informed of the school expectations regarding safe and appropriate use
 (e.g. not sharing passwords or sharing images) prior to being given access.

8. Responding to Online Incidents and Safeguarding Concerns

- All members of the community will be made aware of the range of online risks that are likely to be encountered, including sexting, online/cyber bullying etc. This will be highlighted within staff training and educational approaches for pupils.
- All members of the school community will be informed about the procedure for reporting online safety concerns, such as breaches of filtering, sexting, cyberbullying, illegal content etc.
- The Designated Safeguarding Lead/s (DSL) will be informed of any online safety incidents involving child protection concerns, which will then be recorded.
- The DSLs will ensure that online safety concerns are escalated and reported to relevant agencies in line with the West Sussex Safeguarding Children Board thresholds and procedures.
- Complaints about internet misuse will be dealt with under the school's complaints procedure.
- Complaints about online/cyber bullying will be dealt with under the school's Anti-bullying policy and procedure
- Any complaint about staff misuse will be referred to the Headteacher.
- Any allegations against a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- Pupils, parents and staff will be informed of the school's complaints procedure.
- Staff will be informed of the complaints and whistleblowing procedure.
- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.
- The school will manage online safety incidents in accordance with the school Discipline/Behaviour policy, where appropriate.
- The school will inform parents/carers of any incidents or concerns as and when required.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes as required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place, then the school will contact the Education Safeguards Team or Sussex Police via 101 or 999 if there is immediate danger or risk of harm.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Sussex Police.

- If the school is unsure of how to proceed with any incidents of concern, then the incident will be escalated to the Education Safeguarding Team.
- If an incident of concern needs to be passed beyond the school community, then the concern will be escalated to the Education Safeguarding Team to communicate to other schools in West Sussex.
- Parents and children will need to work in partnership with the school to resolve issues.

9. Procedures for Responding to Specific Online Incidents or Concerns

9.1 Responding to concerns regarding Youth Produced Sexual Imagery (YPSI) or 'Sexting':

- Ashurst Primary School endeavours to ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of sharing, possessing and creating youth produced sexual imagery (known as 'sexting').
- The school will implement preventative approaches via a range of age and ability appropriate educational approaches for pupils, staff and parents/carers.
- Ashurst Primary School views 'sexting' as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Leads (DSL).
- The school will follow the guidance as set out in the non-statutory UKCCIS advice 'Sexting
 in schools and colleges: responding to incidents and safeguarding young people' and WSSCB
 "Responding to youth produced sexual imagery" guidance.
- If the school are made aware of incident involving creating youth produced sexual imagery the school will:
 - Act in accordance with the school's Child Protection and Safeguarding policy and the relevant West Sussex Safeguarding Child Boards procedures
 - o Immediately notify the Designated Safeguarding Lead.
 - o Store the device securely
 - o Carry out a risk assessment in relation to the child/children involved
 - Consider the vulnerabilities of pupil/s involved (including carrying out relevant checks with other agencies)
 - Make a referral to children's social care and/or the police (as needed/appropriate)
 - Put the necessary safeguards in place for pupils, e.g. offer counselling support and immediate protection, and offer appropriate pastoral support for those involved
 - Implement appropriate sanctions in accordance with the school's Behaviour policy, but taking care not to further traumatise victims where possible
 - Review the handling of any incidents to ensure that the school is implementing best practice and the Leadership Team will review and update any management procedures where necessary

- o Inform parents/carers about the incident and how it is being managed.
- The school will not view any images suspected of being youth produced sexual imagery unless there is no other possible option or there is a clear need or reason to do so (in these cases the image will only be viewed by the Designated Safeguarding Lead).
- The school will not send, share or save content suspected to be an indecent image of children and will not allow or request children to do so.
- If an indecent image has been taken or shared on the school network or devices, then the school will take action to block access to all users and isolate the image.
- The school will take action regarding creating youth produced sexual imagery, regardless of the use of school equipment or personal equipment, both on and off the premises.
- The school will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.

9.2 Responding to concerns regarding Online Child Sexual Abuse and Exploitation (CSAE):

- Ashurst Primary School will ensure that all members of the community are made aware of online child sexual abuse, e.g. exploitation and grooming, including the consequences, possible approaches which may be employed by offenders to target children and how to respond to concerns.
- The school will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate educational approaches for pupils, staff and parents/carers.
- Ashurst Primary School views online child sexual abuse as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Leads (DSL).
- If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Sussex Police.
- If the school is made aware of intelligence or information which may relate to child sexual exploitation (on or offline), then it will be passed through to the CSET team by the DSLs.
- If the school are made aware of an incident involving online child sexual abuse of a child then the school will:
 - Act in accordance with the school's Child Protection and Safeguarding policy and the relevant West Sussex Safeguarding Child Boards procedures
 - \circ Immediately notify the Designated Safeguarding Lead
 - Store any devices involved securely
 - o Immediately inform Sussex Police via 101 (using 999 if a child is at immediate risk)
 - Where appropriate, the school will involve and empower children to report concerns regarding online child sexual abuse e.g. using the Click CEOP report form: www.ceop.police.uk/safety-centre/

- Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies)
- Make a referral to children's social care (if needed/appropriate)
- Put the necessary safeguards in place for pupil/s, e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved
- o Inform parents/carers about the incident and how it is being managed
- Review the handling of any incidents to ensure that the school is implementing best practice and the school Leadership Team will review and update any management procedures where necessary.
- The school will take action regarding online child sexual abuse, regardless of the use of school equipment or personal equipment, both on and off the school premises.
- The school will ensure that all members of the community are aware of sources of support regarding online child sexual abuse.
- If pupils at other schools are believed to have been targeted then the school will seek support from the Education Safeguarding Team to enable other schools to take appropriate action to safeguarding their community.
- The school will ensure that the Click CEOP report button is visible and available to pupils and other members of the school community, for example including the CEOP 'report' button on the school website homepage and on intranet systems.

9.3 Responding to concerns regarding Indecent Images of Children (IIOC):

- Ashurst CE Primary School will ensure that all members of the community are made aware
 of the criminal nature of Indecent Images of Children (IIOC), including the possible
 consequences.
- The school will take action regarding of Indecent Images of Children (IIOC) regardless of the use of school equipment or personal equipment, both on and off the premises.
- The school will take action to prevent accidental access to Indecent Images of Children (IIOC), for example, using an Internet Service Provider (ISP) which subscribes to the Internet Watch Foundation block list, implementing appropriate web filtering, implementing firewalls and anti-spam software.
- If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead/s will obtain advice immediately through the Education Safeguarding Team and/or Sussex Police.
- If the school is made aware of Indecent Images of Children (IIOC) then the school will:
 - Act in accordance with the schools Child Protection and Safeguarding policy and the relevant West Sussex Safeguarding Child Boards procedures
 - o Immediately notify the school Designated Safeguard Lead/s (DSL)

- Store any devices involved securely
- o Immediately inform appropriate organisations, e.g. the Internet Watch Foundation (IWF), Sussex Police via 101 (using 999 if a child is at immediate risk) and/or the LADO (if there is an allegation against a member of staff).
- If the school is made aware that a member of staff or a pupil has been inadvertently exposed to indecent images of children whilst using the internet then the school will:
 - Ensure that the Designated Safeguard Lead/s is/are informed
 - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk
 - o Ensure that any copies that exist of the image, for example in emails, are deleted.
- If the school are made aware that indecent images of children have been found on the school's electronic devices then the school will:
 - o Ensure that the Designated Safeguard Lead/s is/are informed
 - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk
 - o Ensure that any copies that exist of the image, for example in emails, are deleted
 - o Inform the Sussex Police via 101 (999 if there is an immediate risk of harm) and children's social services, as appropriate
 - Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
- If the school are made aware that a member of staff is found in possession of indecent images of children on their electronic device provided by the school, then the school will:
 - Ensure that the Designated Safeguard Lead/s is/are informed or another member of staff in accordance with the school whistleblowing procedure
 - Contact Sussex Police regarding the images and quarantine any devices involved until police advice has been sought
 - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with the schools managing allegations policy
 - o Follow the appropriate school policies regarding conduct.

9.4 Responding to concerns regarding radicalisation and extremism online:

- The school will take all reasonable precautions to ensure that pupils are safe from terrorist and extremist material when accessing the internet in schools, and that suitable filtering is in place which takes into account the needs of pupils.
- When concerns are noted by staff that a child may be at risk of radicalisation online, then the Designated Safeguarding Lead (DSL) will be informed immediately and action will be taken in line with the safeguarding policy.

 Online hate content directed towards or posted by specific members of the community will be responded to in line with existing school policies, including Anti-bullying, Behaviour etc. If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately via the Education Safeguarding Team and/or Sussex Police.

9.5 Responding to concerns regarding cyberbullying:

- Cyberbullying, along with all other forms of bullying, of any member of the Ashurst Primary School community will not be tolerated. Full details are set out in the school policies regarding Anti-bullying and Behaviour.
- All incidents of online bullying reported will be recorded.
- There are clear procedures in place to investigate incidents or allegations and support anyone in the school community affected by online bullying. All members of the community will be advised to report online hate in accordance with relevant school policies and procedures e.g. Anti-bullying, Behaviour etc.
- If the school is unclear if a criminal offence has been committed, then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Sussex Police.
- Pupils, staff and parents/carers will be advised to keep a record of cyberbullying as evidence.
- The school will take steps to identify the bully where possible and appropriate. This
 may include examining school system logs, identifying and interviewing possible
 witnesses, and contacting the service provider and the police, if necessary.
- Pupils, staff and parents/carers will be required to work with the school to support the
 approach to cyberbullying and the school's online safety ethos.
- Sanctions for those involved in online or cyberbullying may include:
 - Those involved will be asked to remove any material deemed to be inappropriate or offensive
 - A service provider may be contacted to remove content if those involved refuse to or are unable to delete content
 - Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools Antibullying, Behaviour or Acceptable Use Policy
 - o Parent/carers of pupils involved in online bullying will be informed
 - o The Police will be contacted if a criminal offence is suspected.

The Designated Safeguarding Leads (DSL) are Mrs Janet Williams, (Headteacher, SENCO & DSL Lead), Mrs Amanda Hedley (DSL E-Learning, Network Manager, Computing teacher & Office Admin) Mrs S Smith (DSL & Lead Teacher) and Mrs Tina Clarke (DSL & FS/KS1 Teacher).

The Online safety lead for the Governing Body is the Chair of Governors.

Reviewed, Adopted and Ratified by: Staff: January 2020 Governing Body: (date)

Date for Review: September 2021

APPENDIX A

E-Safety Contacts and References

West Sussex Support and Guidance:

West Sussex County Council (Schools): www.schools.westsussex.gov.uk/

West Sussex Safeguarding Children Board (WSSCB): www.westsussexscb.org.uk/

E-Safety in West Sussex Schools:

www.westsussex.gov.uk/learning/west_sussex_grid_for_learning/management_info__services/it_support_for_schools/e-safety_in_west_sussex_school.aspx

Pan Sussex E-Safety Strategy: http://www.westsussexscb.org.uk/wp-content/uploads/Pan-Sussex-E-safety-strategy.pdf

A Guide To Keeping Your Child Safe Online: https://www.westsussex.gov.uk/media/8523/online-safety-completed.pdf

Sussex Police:

www.sussex.police.uk/

In an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries contact Sussex Police via 101

National Links and Resources:

Action Fraud: www.actionfraud.police.uk BBC WebWise: www.bbc.co.uk/webwise

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk

ChildLine: www.childline.org.uk Childnet: www.childnet.com

Get Safe Online: www.getsafeonline.org
Internet Matters: www.internetmatters.org

Internet Watch Foundation (IWF): www.iwf.org.uk Lucy Faithfull Foundation: www.lucyfaithfull.org

Know the Net: www.knowthenet.org.uk

National Online Safety: www.nationalonlinesafety.com/

Net Aware: www.net-aware.org.uk NSPCC: www.nspcc.org.uk/onlinesafety Parent Port: www.parentport.org.uk

Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline

The Marie Collins Foundation: www.mariecollinsfoundation.org.uk/

Think U Know: www.thinkuknow.co.uk

Virtual Global Taskforce: www.virtualglobaltaskforce.com UK Safer Internet Centre: www.saferinternet.org.uk

360 Safe Self-Review Tool for Schools: www.360safe.org.uk/

Online Compass (Self review tool for other settings): www.onlinecompass.org.uk/

Appendix C – Children Requiring Mental Health Support

- 1. We recognise our school has an important role to play in supporting the mental health and wellbeing of our pupils.
- 2. We recognise mental health problems can, in some cases, be an indicator that a child has suffered or is at risk of suffering abuse, neglect or exploitation.

Ashurst CE Aided Primary School's Emotional Well-being Lead is Mrs T Clarke Stress Management Lead is Mrs A Hedley

- 1. As a school we will have a clear system and process in place for identifying possible mental health problems, including routes to escalate and clear referral and accountability systems. We will make sure all staff and volunteers are aware of our system.
- 2. Where there are concerns about the mental health, wellbeing and safeguarding of a child, staff will immediately discuss those concerns with the Designated Safeguarding Lead.
- 3. We are aware of recent government publications:

- Preventing and tackling bullying, 6
- Mental health and behaviour in schools, 7 and
- Promoting children and young people's emotional health and wellbeing⁸.
- 4. Our staff are aware of the West Sussex Community Mental Health Liaison Service https://www.sussexpartnership.nhs.uk/west-sussex-cmhl-service#:~:text=The%20new%20Community%20Mental%20Health,to%20moderate%20mental%20health%20conditions who provide an early intervention and prevention service for professionals who are working with young people under the age of 18, and are concerned about a young person's mental health and wellbeing. This service is available to our school.
- 5. We are aware that we can obtain advice and support from School Nursing Service https://www.sussexcommunity.nhs.uk/downloads/services/west-sussex-school-nursing/west-sussex-school-nursing-leaflet.pdf
- 6. We are also aware of the resources available to our school from the Mentally Healthy Schools website https://www.mentallyhealthyschools.org.uk/
- 7. N/A For our pupils aged 11-19 we are aware of the <u>ChatHealth</u> text service and <u>YES Youth</u> <u>Emotional Support Service</u>

Self-Harm Guidance for Schools

Managing self-harm guidance and tool kit for schools in West Sussex has recently been created with the latest information and resources to help recognise the signs, identify risks and access the support available.

We recognise that <u>Self-Harm Guidance for schools</u> is available to anyone working in education, to support staff when dealing with students who self-harm, or are at risk of intentionally harming themselves.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/623895/Preventing_a nd_tackling_bullying_advice.pdf

⁶

⁷ https://www.gov.uk/government/publications/mental-health-and-behaviour-in-schools--2

⁸ https://www.gov.uk/government/publications/promoting-children-and-young-peoples-emotional-health-and-wellbeing