ASTON-ON-TRENT PRIMARY SCHOOL

ONLINE SAFETY POLICY

School policy, reviewed and approved by Governors on 9th November 2026

This policy has been impact assessed in the light of all other school policies, including the Disability Equality Scheme.

SIGNED:	PRINT NAME:	DATE:
	C. Coles Chair of Governors	09.11.26
SIGNED:	**PRINT NAME:**	**DATE:**
	S. Moore Headteacher	09.11.26

Document name	Online Safety Policy
Document owner	Aston on Trent Primary School
Authors	The education people, Kent County Council, Derbyshire County – CPM Schools/Education
Date approved & rectified	21h October 2026
Review date	
Headteacher/Principal	Mr Sam Moore
Link Governor	Clare Coles

Designated Safeguarding Lead: Sam Moore; Katie Baxter; Nick Snow
Named Governor with lead responsibility: Clare Coles
Named teacher with responsibility for Computing: Emma Dawes
Named teacher with responsibility for PSHE : Sam Moore / Jess Baird

School website link to online safety - Online Safety

Aston on Trent Primary School Online Safety Policy

Contents

	Page no
Using the Online Safety Policy Template	3
1. Policy Aims	5
2. Policy Scope	5
2.2 Links with other policies and practices	6
3. Monitoring and Review	6
4. Roles and Responsibilities	6
4.2 The leadership and management team	6
4.3 The Designated Safeguarding Lead	7
4.4 Members of staff	8
4.5 Staff who manage the technical environment	8
4.6 Learners	8
4.7 Parents	9
5. Education and Engagement Approaches	9
5.2 Education and engagement with learners	9
5.3 Vulnerable Learners	10
5.4 Training and engagement with staff	10
5.5 Awareness and engagement with parents	11
6. Reducing Online Risks	11
7. Safer Use of Technology	12
7.2 Classroom Use	12
7.3 Managing Internet Access	13
7.4 Filtering and Monitoring	13
7.5 Managing Personal Data Online	14
7.6 Security and Management of Information Systems	14
7.7 Managing the Safety of the Website	15
7.8 Publishing Images and Videos Online	15
7.9 Managing Email	15
Educational use of Videoconferencing and/or Webcams	16
7.10 Management of Learning Platforms	17
7.11 Management of Applications (apps) used to Record Learners Progress	18
8. Social Media	18
8.2 Expectations	18
8.3 Learners Personal Use of Social Media	20
8.4 Official Use of Social Media	21
9. Use of Personal Devices and Mobile Phones	22
9.2 Expectations	22

9.3 Staff Use of Personal Devices and Mobile Phones 23
9.4 Learners Use of Personal Devices and Mobile Phones 23
9.5 Visitors' Use of Personal Devices and Mobile Phones 24
10. Responding to Online Safety Incidents and Concerns 25
10.2 Concerns about Learner Welfare 25
11. Procedures for Responding to Specific Online Incidents or Concerns 26
11.2 Online Sexual Violence and Sexual Harassment between Children 26
11.3 Youth Produced Sexual Imagery or "Sexting" 27
11.4 Online Child Sexual Abuse and Exploitation 28
11.5 Indecent Images of Children (IIOC) 29
11.6 Cyberbullying 30
11.7 Online Hate 30
11.8 Online Radicalisation and Extremism 31
12. Useful Links for Educational Settings 32

Policy Aims

- This online safety policy has been written by Aston on Trent Primary School, involving staff, learners and parents/carers, building on the Kent County Council/The Education People online safety policy template, with specialist advice and input, and reformatted and with additions, with permission by the Child Protection Manager for schools/education, Derbyshire county council as required.

- It takes into account the DfE statutory guidance 'Keeping Children Safe in Education' , Early Years and Foundation Stage (insert only if applicable) 'Working Together to Safeguard Children' and the Derby and Derbyshire Safeguarding Children Partnership Safeguarding procedures.

- The purpose of this online safety policy is to:
    - Safeguard and protect all members of Aston on Trent Primary School community online.
    - Identify approaches to educate and raise awareness of online safety throughout the community.
    - Enable all staff to work safely and responsibly, including in the delivery of remote learning, to role model positive behaviour online and to manage professional standards and practice when using technology.
    - Identify clear procedures to use when responding to online safety concerns.

- This school identifies that the issues classified within online safety are considerable, but can be broadly categorised into four areas of risk:
    - **Content:** being exposed to illegal, inappropriate or harmful material
    - **Contact:** being subjected to harmful online interaction with other users
    - **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm.
    - **Commerce:** risk associated with online commercial activity, including advertising, in-app purchases, scams, phishing, financial exploitation and inappropriate spending of money online.

1. Policy Scope

- Aston on Trent Primary School believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all learners and staff are protected from potential harm online.
- Aston on Trent Primary School identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life.
- Aston on Trent Primary School believes that learners should be empowered to build resilience and to develop strategies to manage and respond to risk online.
- This policy applies to all staff including the governing body, leadership team, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the setting (collectively referred to as "staff" in this policy) as well as learners, parents and carers.
- This policy applies to all access to the internet and use of technology, including personal devices, or where learners, staff or other individuals have been provided with setting issued devices for use off-site, such as a work laptops, tablets or mobile phones.

1.2 Links with other policies and practices

This policy links with several other policies, practices and action plans including:

- Anti-bullying policy
- Acceptable Use Policies (AUP) and/or the Code of conduct/staff behaviour policy
- Behaviour and discipline policy
- Confidentiality policy
- Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE), Citizenship and Relationships and Sex Education (RSE)
- Data security
- Image use policy
- Mobile phone and social media policies
- Safeguarding and Child protection policy
- Searching, screening and confiscation policy

2. Monitoring and Review

- Technology in this area evolves and changes rapidly. This school will review this policy at least annually.
  - The policy will also be revised following any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure.
- We will regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.
- To ensure they have oversight of online safety, the Head teacher will be informed of online safety concerns, as appropriate.
- The named governor for safeguarding will report on a regular basis to the governing body on online safety practice and incidents, including outcomes.
- Any issues identified via monitoring will be incorporated into our action planning.

3. Roles and Responsibilities

- The Designated Safeguarding Lead (DSL) (Mr Moore, head teacher) has lead responsibility for online safety. ***Whilst activities of the designated safeguarding lead may be delegated to an appropriately trained deputy, overall the ultimate lead responsibility for safeguarding and child protection, including online safety remains with the DSL***.
- Aston on Trent Primary School recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

4.1 The leadership and management team will:

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Ensure there are appropriate and up-to-date policies regarding online safety; including a staff code of conduct/behaviour policy *and* acceptable use policy, which covers use of technology.

- Ensure that suitable and appropriate filtering and monitoring systems are in place and work with technical staff to monitor the safety and security of our systems and networks.
- Ensure that online safety is embedded within a progressive curriculum, which enables all learners to develop an age-appropriate understanding of online safety.
- Support the DSL and any deputies by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.
- Ensure parents are directed to online safety advice and information
- Provide information on a school's website for parents and the community
- Ensure there are robust reporting channels for the community to access regarding online safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology.
- Audit and evaluate online safety practice to identify strengths and areas for improvement.

4.2 The Designated Safeguarding Lead (DSL) will:

- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
- Work alongside deputy DSLs to ensure online safety is recognised as part of the settings safeguarding responsibilities and that a coordinated approach is implemented.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training.
- Access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant knowledge and up to date required to keep learners safe online.
- Access regular and appropriate training and support to ensure they recognise the additional risks that learners with SEN and disabilities (SEND) face online.
- Keep up-to-date with current research, legislation and trends regarding online safety and communicate this with the community, as appropriate.
- Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
- Ensure that online safety is promoted to parents, carers and the wider community, through a variety of channels and approaches.
- Maintain records of online safety concerns, as well as actions taken, as part of the settings safeguarding recording mechanisms.
- Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures.
- Report online safety concerns, as appropriate, to the setting management team and Governing Body.
- Work with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input.
- Meet regularly (termly) with the governor with a lead responsibility for safeguarding *and* online safety.

4.3 It is the responsibility of all members of staff to:

- Contribute to the development of online safety policies.
- Read and adhere to the online safety policy and acceptable use policies.
- Take responsibility for the security of setting systems and the data they use or have access to.
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.
- Embed online safety education in curriculum delivery, wherever possible.
- Have an awareness of a range of online safety issues and how they may be experienced by the children in their care.
- Identify online safety concerns and take appropriate action by following the settings safeguarding policies and procedures.
- Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.

- Identify students who are involved in cybercrime, or those who are technically gifted and talented and are at risk of becoming involved in cybercrime, and make a Cyber Choices referral.

4.4 It is the responsibility of staff managing the technical environment 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.
- Implement appropriate security measures as directed by the DSL and leadership team *(*see Acceptable Use of ICT policy and section 7 below) to ensure that the settings IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensure that our filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- Ensure that our monitoring systems are applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team
- Ensure appropriate access and technical support is given to the DSL (and/or deputy) to our filtering and monitoring systems, to enable them to take appropriate safeguarding action if/when required.

4.5 It is the responsibility of learners (at a level that is appropriate to their individual age and ability) to:

- Engage in age appropriate online safety education opportunities.
- Contribute to the development of online safety policies.
- Read and adhere to the acceptable use policies.
- Respect the feelings and rights of others both on and offline.
- Take responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues.
- Report online content, contact, conduct or commerce concerns to a trusted adult.
- Protect their personal information and respect the privacy of others when using digital technologies.
- Use technology, including emerging technologies such as artificial intelligence (AI), safely, responsibly and in accordance with school expectations.
- Consider the reliability of information found online and seek support if they are unsure whether content is trustworthy.

4.6 It is the responsibility of parents and carers to:

- Read the acceptable use policies and encourage their children to adhere to them.
- Support our online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home.
- Role model safe and appropriate use of technology and social media.
- Abide by the home-school agreement *and* acceptable use policies.
- Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the setting, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Contribute to the development of the online safety policies.
- Use our systems, such as learning platforms, and other network resources, safely and appropriately.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.
- Report online safety concerns to school and work in partnership with the school to address issues affecting their child.
- Encourage their child to protect personal information and use technology safely, responsible and respectfully.
- Support their child in developing critical thinking skills when accessing online information and help them to recognize misinformation, disinformation and online scams.

5. Education and Engagement Approaches

5.1 Education and engagement with learners

- The setting will establish and embed a progressive online safety curriculum to raise awareness and promote safe and responsible internet use amongst learners by:
    - Ensuring education regarding safe and responsible use precedes internet access.
    - Including online safety in Personal, Social, Health and Economic (PSHE), Relationships and Sex Education (RSE) and computing programmes of study
    - or the internet is in use.
    - Educating learners in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
    - Teaching learners to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
    - Teaching learners to recognize and safely use emerging technologies, including artificial intelligence (AI), and to understand the risks associated with AI- generated content, misinformation and disinformation.Ensuring learners understand online risks relating to content, contact, conduct and harmful online behaviour.
    - Teaching learners how to report online safety concerns, inappropriate content and harmful online behaviours.
    - Teaching learners how to protect personal information, respect the privacy of others and manage their digital footprint responsibly.

- The setting will support learners to read and understand the acceptable use policies in a way which suits their age and ability by:
    - Displaying acceptable use posters in all rooms with internet access.
    - Informing learners that the use of school devices, networks and online services may be filtered and monitored to support safeguarding, security and compliance with data protection legislation.
    - Rewarding positive use of technology.
    - Implementing appropriate peer education approaches.
    - Providing online safety education and training as part of the transition programme across the key stages and when moving between establishments.
    - Seeking learner voice when writing and developing online safety policies and practices, including curriculum development and implementation.
    - Using support, such as external visitors, where appropriate, to complement and support our internal online safety education approaches.

5.2 Vulnerable Learners

- Aston on Trent Primary School recognises that some learners are more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND), children with social emotional or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss, and children who may be vulnerable to exploitation or abuse.
- Aston on Trent Primary School will ensure that online safety education, access and

support are adapted, differentiated and made accessible to meet the needs of all learners, including those identified as vulnerable.

- When implementing an appropriate online safety policy and curriculum Aston on Trent Primary School will seek input from specialist staff as appropriate, including the SENCO, Child in Care Designated Teacher and where appropriate, external agencies and professionals.

5.3 Training and engagement with staff

We will:

- Provide and discuss the online safety policy and procedures with all members of staff as part of induction.
- Provide up-to-date and appropriate online safety training for all staff, including governors where relevant to their role on a regular basis, with at least annual updates.
    - Annual Safeguarding training every September led by the DSL or deputy DSL. LA training bi-annually. Safeguarding induction training for all staff/volunteers led by DSL or deputy DSL. Bi-annual online safety training for pupils/staff/parents/Governors.
    - This will cover the potential risks posed to learners through online content, contact, conduct and commerce, as well as emerging risks associated with the use of social media, online gaming, livestreaming, artificial intelligence (AI) and misinformation.
- Recognise the expertise staff build by undertaking safeguarding training and managing safeguarding concerns and provide opportunities for staff to contribute to and shape online safety policies and procedures.
- Ensure all staff receive appropriate training regarding the school's filtering and monitoring systems, including how to identify, report and respond to safeguarding concerns identified through these systems.
- Make staff aware that our IT systems are monitored, and that activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices.
- Make staff aware that their online conduct outside of the setting, including personal use of social media, could have an impact on their professional role and reputation.
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the learners.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting learners, colleagues or other members of the community.

5.4 Awareness and engagement with parents and carers

- Aston on Trent Primary School recognises that parents and carers have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies.
- We will build a partnership approach to online safety with parents and carers by:
    - Providing advice, guidance and resources to help parents and carers support the safe, responsible and age-appropriate use of technology, social media, gaming platforms and emerging technologies, including artificial intelligence (AI)
    - Raising awareness of online risks relating to content, contact, conduct and commerce and how parents and carers can help children manage these risks safely.
    - Signposting parents and carers to appropriate local and national sources of online safety information, support and advice.
    - Encouraging parents and carers to report online safety concerns to the school and to work in partnership with staff to address issues affecting learners.
    - Providing information about the school's filtering and monitoring approaches where appropriate, to support a shared understanding of online safeguarding responsibilities.
    - Requiring parents and carers to read and support our acceptable use policies and discuss the expectations for safe and responsible technology use with their children.

6. Reducing Online Risks

- Aston on Trent Primary School recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace.
- We will:
    - Regularly review the methods used to identify, assess and minimise online risks.
    - Examine emerging technologies, including artificial intelligence (AI), for educational benefit and undertake appropriate risk assessments before use in the setting is permitted.
    - Consider online safety, safeguarding and data protection risks when introducing new technologies, platforms, applications or online services.
    - Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.
    - Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via our computers or devices.
- All members of the community are made aware of our expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community.

This is clearly outlined in our acceptable use policies and highlighted through a variety of education and training approaches.

7. Safer Use of Technology

7.1 Classroom Use

- Aston on Trent Primary School uses a wide range of technology. This includes access to:
  - Computers, laptops and other digital devices
  - Internet which may include search engines and educational websites
  - Learning platform/intranet
  - Email
  - Games consoles and other games-based technologies
  - Digital cameras, web cams and video cameras
- All setting owned devices will be used in accordance with our acceptable use policies and with appropriate safety and security measures in place.
- Members of staff will evaluate the educational value, safeguarding implications, data protection requirements and age appropriateness of websites, apps, online services and emerging technologies, including artificial intelligence (AI), before use within the setting.
- The setting will use age-appropriate search tools following an informed risk assessment, to identify which tool best suits the needs of our community.
- The search tools suggested for staff and learners to use are:
  - Google Safe Search
  - Google (for staff)
- We will ensure that the use of internet-derived materials, by staff and learners complies with copyright law and acknowledge the source of information.
- Supervision of learners will be appropriate to their age and ability.
  - **Early Years Foundation Stage and Key Stage 1**
    - Access to the internet will be by adult demonstration, with occasional directly supervised access to specific and approved online materials, which supports the learning outcomes planned for the learners age and ability.
  - **Key Stage 2**
    - Learners will use age-appropriate search engines and online tools.
    - Learners will be directed by the teacher to online materials and resources which support the learning outcomes planned for the learners age and ability.

7.2 Managing Internet Access

- We will maintain a written record of users who are granted access to our devices and systems.
- All staff, learners and visitors will read and sign an acceptable use policy before being given access to our computer system, IT resources or internet.
- Access to school systems and online services will be managed appropriately and reviewed when required.
- The school will ensure appropriate filtering and monitoring systems are in place to support safeguarding and identify potential online safety concerns.
- We will carry out regular monitoring and review activities to evaluate the effectiveness of

our filtering and monitoring arrangements and to identify any safeguarding concerns, inappropriate access attempts or system vulnerabilities.

- Any concerns identified through filtering, monitoring or audit activities will be managed in line with the school's safeguarding, behaviour and child protection procedures.

7.3 Filtering and Monitoring

Note: A guide for education settings about establishing 'appropriate levels' of filtering and monitoring can be found at: *https://www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/appropriate-filtering-and-monitoring*

7.3.1 Decision Making

- Aston on Trent Primary School governors and leaders have ensured that our setting has age and ability appropriate filtering and monitoring in place, to limit learner's exposure to online risks.
- The governors and leaders are aware of the need to prevent "over blocking", as that may unreasonably restrict what can be taught, with regards to online activities and safeguarding.
- Our decision regarding filtering and monitoring has been informed by a risk assessment, considering our specific needs and circumstances.
- Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from the leadership team; all changes to the filtering policy are logged and recorded.
- The leadership team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.
- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard learners; effective classroom management and regular education about safe and responsible use is essential.

7.3.2 Filtering

- Education broadband connectivity is provided through Wave9.
- We use Wave9 filtering systems to restrict access to content that is illegal, inappropriate or harmful to children and young people. Categories of content blocked may include, but are not limited to, violence, extremism, hate content, illegal activities, gambling or other inappropriate material.
- The filtering system blocks all sites on the Internet Watch Foundation (IWF) list.
- Filtering systems are regularly reviewed to ensure they remain effective, appropriate and proportionate to the age and needs of our learners.
- We work with Wave9 to ensure that our filtering policy is continually reviewed.
- If learners discover unsuitable sites, they will be required to:
    - Report the concern immediately to a member of staff
    - The member of staff will report the concern (including the URL of the site if possible) to the DSL (or deputy) and/or technical staff.
    - The breach will be recorded and escalated as appropriate.
    - Parents/carers will be informed of filtering breaches involving their child where

appropriate.

- Any material suspected to be illegal, harmful or indicative of a safeguarding concern will be reported immediately to the appropriate agencies and managed in accordance with safeguarding procedures. This may include referral to organisations such as the Internet Watch Foundation (IWF), CEOP, the police or children's social care, where appropriate.

7.3.4 Monitoring

- We will appropriately monitor the use of school devices, networks and online services to safeguard learners and staff, maintain network security and support the effective operation of our system.
- This is achieved through:
    - Appropriate staff supervision when learners are using internet-enabled devices and online services
    - Monitoring internet and web access through the review of logs, reports and alerts generated by our systems.
    - Monitoring activity on school devices, networks and online services where appropriate and proportionate.
- Monitoring arrangements are regularly reviewed to ensure they remain effective, appropriate and proportionate to the needs of the school community.
- If a concern is identified through monitoring approaches:
    - The concern will be reviewed by the appropriate member of staff
    - Safeguarding concerns will be reported to the DSL or Deputy DSL without delay.
    - The DSL or Deputy DSL will respond in line with the Child Protection and Safeguarding Policy.
    - Incidents will be recorded and managed in accordance with the school's safeguarding, behaviour and data protection procedures.
- All users will be informed that use of school devices, systems and online services may be monitored and that monitoring will be undertaken in accordance with data protection, human rights and privacy legislation.
- All staff are aware that filtering and monitoring systems form part of the school's safeguarding arrangements and do not replace effective supervision, classroom management and online safety education.

7.4 Managing Personal Data Online

- Personal data will be collected, recorded, stored, processed, transferred and shared securely in accordance with UK data protection legislation, including the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and any subsequent amendments.

    - Further information can be found within the school's Information Security Policy and Data Protection Policy.

7.5 Security and Management of Information Systems

- We take appropriate steps to ensure the security of our information systems, including:
    - Virus protection being updated regularly.
    - Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
    - Not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use.
    - Not downloading unapproved software to work devices or opening unfamiliar email attachments.
    - Regularly reviewing and monitoring systems, files and network activity, where appropriate, to identify security vulnerabilities and potential safeguarding.
    - The secure use of individual user accounts, passwords and authentication methods to access school systems and networks.
        - Individual user accounts and passwords will be provided and enforced for all users; account credentials must not be shared.
    - All users are expected to log off or lock their screens/devices if systems are unattended.
    - Access to personal data and school systems will be restricted to authorized users according to their role and responsibilities.
    - Any suspected data breach, cyber security incident or unauthorised access to information will be reported and managed in accordance with the school's data protection and incident management procedures.
    - Appropriate backup and recovery procedures will be in place to minimize the impact of data loss, system failure or cyber incidents.
    - Further information about technical environment safety and security can be found at:
        - Acceptable Use of ICT

7.5.1 Password policy

- All members of staff will have their own unique username and private passwords to access our systems; members of staff are responsible for keeping their password confidential and secure.
- Where online recording systems are used, including child protection recording systems, access will be restricted according to job role and responsibilities and reviewed regularly.
- From Reception, all learners are provided with their own unique username and private passwords to access our systems; learners will be supported to keep their login credentials secure and private.
- We require all users to:
    - Use strong passwords for access into our system - the longer and more unusual, the stronger it becomes. Using a combination of upper, lower case, numbers and special characters is recommended.
    - Keep passwords confidential and not share them with others.
    - Report any suspected compromise of account details immediately.
    - Change passwords promptly if there is a reason to believe they have been compromised.

- Lock or log off devices when systems are left unattended.
- Use multi-factor authentication where available and appropriate.
- Not to login as another user at any time.

7.6 Managing the Safety of our Website

- We will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE).
- We will ensure that our website complies with guidelines for publications including: accessibility; data protection; respect for intellectual property rights; privacy policies and copyright.
- Staff or learner's personal information will not be published on our website; the contact details on the website will be our setting address, email and telephone number.
- The administrator account for our website will be secured with an appropriately strong password.
- We will post appropriate information about safeguarding, including online safety, on our website for members of the community.

7.7 Publishing Images and Videos Online

- We will ensure that all images and videos shared online are used in accordance with the associated policies, including (but not limited to) the cameras and image use, data security, acceptable use, staff code of conduct, social media, and use of personal devices and mobile phones policies.
- Images and videos of learners will only be published where appropriate consent has been obtained and in accordance with the school's data protection and image use policies.
- Images and videos shared online will be carefully reviewed to ensure they do not compromise the privacy, dignity, safety or wellbeing of learners and staff.
- Personal information will not be published alongside images or videos where doing so may increase safeguarding or privacy risks.
- Staff will ensure that images and videos are stored, transferred and shared securely in accordance with the school's information security and data protection procedures.

7.8 Managing Email

- Access to our email systems will always take place in accordance with data protection legislation and in line with other policies, including confidentiality, acceptable use policies and the code of conduct/behaviour policy.
  - The forwarding of any chain messages/emails is not permitted.
  - Spam or junk mail will be blocked and reported to the email provider.
  - Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.
  - Setting email addresses and other official contact details will not be used for setting up personal social media accounts.
- Members of the community will immediately tell Mr Moore, DSL, if they receive offensive communication, and this will be recorded in our safeguarding files/records.
- We will have a dedicated email for reporting wellbeing and pastoral issues. This inbox will be

managed by designated and trained staff.

7.8.1 Staff email

- Staff will use school-provided email accounts for all professional communication with parents/carers and external agencies unless otherwise authorised.
- Staff will maintain professional boundaries when communicating electronically and will always follow the staff code of conduct.
- Staff will ensure that personal or sensitive information is only shared in accordance with data protection requirements and school policies.
- Staff will remain vigilant to phishing emails, suspicious messages and cyber security risks and report concerns immediately.
- Email communications should be professional, appropriate and relevant to the purpose of communication.

7.8.2 Learner email

- If learners are provided with email accounts, they are to be used for educational purposes.
- Learners will receive education regarding safe and appropriate email etiquette before access is permitted.

7.9 Educational use of Videoconferencing and/or Webcams

- Aston on Trent Primary School recognise that videoconferencing, webcams and other online communication technologies can provide valuable learning opportunities when used safely, securely and appropriately.
    - All videoconferencing *and/or* webcam equipment will be switched off when not in use and will not be set to auto-answer.
    - Video conferencing equipment connected to the educational broadband network will use the national E.164 numbering system and display their H.323 ID name; external IP addresses will not be made available to other sites.
    - Videoconferencing contact details will not be posted publicly.
    - Videoconferencing equipment will not be taken off the premises without prior permission from the DSL.
    - Staff will ensure that external videoconferencing opportunities and/or tools are suitably risk assessed and will ensure that accounts and systems used to access these events are safe and secure.
    - Video conferencing equipment and webcams will be kept securely and, if necessary, locked away or disabled when not in use.

7.9.1 Users

- Parents/carers consent will be obtained prior to learners taking part in videoconferencing activities.
- Learners will ask permission from a member of staff before making or answering a videoconference call or message.
- Videoconferencing will be supervised appropriately, according to the learner's age and ability.

- Parents are required to be present during video calls

- Video conferencing will take place via official and approved communication channels following a robust risk assessment.
- Only key administrators will be given access to videoconferencing administration areas or remote-control pages.
- The unique log on and password details for the videoconferencing services will only be issued to members of staff and should be kept securely, to prevent unauthorised access.

7.9.2 Content

- When recording a videoconference lesson, it should be made clear to all parties at the start of the conference and written permission will be obtained from all participants; the reason for the recording must be given and recorded material will be stored securely.
- If third party materials are included, we will check that recording is permitted to avoid infringing the third-party intellectual property rights.
- We will establish dialogue with other conference participants before taking part in a videoconference; if it is a non-educational site, staff will check that the material they are delivering is appropriate for the learners.

7.10 Management of Learning Platforms

- Aston on Trent Primary School uses Microsoft Teams as its official learning platform.
- Leaders and staff will regularly monitor the usage of the Learning Platform (LP), including message/communication tools and publishing facilities.
- Only current members of staff, learners and parents will have access to the LP.
- When staff *and/or* learners leave the setting, their account will be disabled or transferred to their new establishment. .
- Learners and staff will be advised about acceptable conduct and use when using the LP.
- All users will be mindful of copyright and will only upload appropriate content onto the LP.
- Any concerns about content on the LP will be recorded and dealt with in the following ways:
  - The user will be asked to remove any material deemed to be inappropriate or offensive.
  - If the user does not comply, the material will be removed by the site administrator.
  - Access to the LP for the user may be suspended.
  - The user will need to discuss the issues with a member of leadership before reinstatement.
  - A learner's parents/carers may be informed.
  - If the content is illegal, we will respond in line with existing child protection procedures.
- Learners may require editorial approval from a member of staff. This may be given to the learner to fulfil a specific aim and may have a limited time frame.
- A visitor may be invited onto the LP by a member of the leadership; in this instance, there may be an agreed focus or a limited time slot.

7.11 Management of Applications (apps) used to Record Children's Progress

- We use HelloData to track learners.

- The *headteacher* is ultimately responsible for the security of any data or images held of children. As such, they will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that they are used in accordance with data protection legislation, including the General Data Protection Regulations (GDPR) and Data Protection legislation.
- To safeguard learner's data:
    - Only learner issued devices will be used for apps that record and store learners' 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 learners' personal details, attainment or images.
    - Devices will be appropriately encrypted if taken off site, to reduce the risk of a data security breach, in the event of loss or theft.
    - All users will be advised regarding safety measures, such as using strong passwords and logging out of systems.
    - Parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images.

8. Social Media

8.1 Expectations

- The expectations' regarding safe and responsible use of social media and remote learning platforms applies to all members of Aston on Trent Primary School community.
- Members of staff will refer to and adhere to the school's social media policy and any other policy where the staff use of social media is referred to.
- We will control learner and staff access to social media whilst using setting provided devices and systems on site.
- Concerns regarding the online conduct of any member of Aston on Trent Primary School community on social media, should be reported to the DSL and will be managed in accordance with our anti-bullying, allegations against staff, behaviour and child protection policies.

8.2 Learners Personal Use of Social Media

- Safe and appropriate use of social media will be taught to learners as part of an embedded and progressive education approach, via age-appropriate sites and resources.
- We are aware that many popular social media sites state that they are not for children under the age of 13, therefore we will not create accounts specifically for learners under this age.
- Any concerns regarding learner's use of social media will be dealt with in accordance with

existing policies, including anti-bullying and behaviour.
    - Concerns will be shared with parents/carers as appropriate, particularly when concerning underage use of social media sites, games or tools.
- Learners will be advised:
    - To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location.
    - To only approve and invite known friends on social media sites and to deny access to others by making profiles private.
    - Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.
    - To use safe passwords.
    - To use social media sites which are appropriate for their age and abilities.
    - How to block and report unwanted communications.
    - How to report concerns both within the setting and externally.

9. Use of Personal Devices and Mobile Phones

- Aston on Trent Primary School recognises that personal communication through mobile technologies, smart devices and other internet-enabled technologies is an accepted part of everyday life for learners, staff and parents/carers. However, these technologies must be used safely, responsibly and in accordance with school policies and procedures.

9.1. Staff Use of Personal Devices and Mobile Phones

- Personal devices will not be used to record, store or share images, videos or personal information relating to learners unless expressly authorised in accordance with school policy.
- Staff will ensure that personal devices are used in a manner which maintains professional boundaries and protects the privacy and wellbeing of learners.
- Personal devices used for work purposes will be secured appropriately, including the use of passwords, PINs or biometric authentication where available.
- Staff will not use personal contact details, social media accounts or messaging services to communicate with learners.

9.2 Learners Use of Personal Devices and Mobile Phones

- Learners will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.
- Aston on Trent Primary School expects learners' personal devices and mobile phones to be handed in (turned off) at the school office on arrival and collected at the end of the school day, where they will be stored securely.
- If a learner needs to contact his/her parents or carers they will be allowed to use a *setting phone*.
    - Parents are advised to contact their child via the setting office.
- Mobile phones or personal devices will not be used by learners during lessons or formal educational time.

- Mobile phones and personal devices must not be taken into examinations.
    - Learners 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 withdrawal from either that examination or all examinations.
- If a learner breaches the policy, the phone or device will be confiscated and will be held in a secure place in the school office.
    - Staff may confiscate a learner's mobile phone or device if they believe it is being used to contravene our behaviour or bullying policy or could contain youth produced sexual imagery (sharing nudes and semi-nudes).
    - Searches of mobile phone or personal devices will only be carried out in accordance with DfE guidance and our policy.
    - Learners mobile phones or devices may be searched by a member of the leadership team, with the consent of the learner or a parent/ carer. Content may be deleted or requested to be deleted, if it contravenes our policies.
    - Mobile phones and devices that have been confiscated will be released to parents or carers at the end of the day.
    - If there is suspicion that material on a learner's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.

9.3 Visitors' Use of Personal Devices and Mobile Phones

- Parents/carers and visitors (including volunteers, contractors and external professionals) must use their mobile phones, personal devices and smart devices in accordance with the school's Acceptable Use Policy and other associated policies, including the Child Protection and Safeguarding, Behaviour, Image Use and Data Protection policies.
- Visitors must not take photographs, videos or audio recordings on site unless authorised by the school and in accordance with school policies.
- We will ensure appropriate signage and information is displayed and provided to inform parents, carers and visitors of expectations of use.
- Members of staff are expected to challenge visitors where appropriate if they have concerns regarding device use and will report any concerns or breaches of policy to the DSL (or Deputy DSL) and/or Headteacher without delay.

9.4 Officially provided mobile phones and devices

- Members of staff will be issued with an email address, where contact with learners or parents/ carers is required.
- Setting devices will be suitably protected via a passcode/password/pin and must only be accessed or used by members of staff.
- Setting devices will always be used in accordance with the acceptable use policy and other relevant policies.
- School-issued devices will be kept secure when not in use and should not be left unattended in public locations.
- Any loss, theft or suspected compromise of a school-issued device will be reported immediately in accordance with the school's data protection and information security procedures.

- Personal or sensitive information stored on school-issued devices will be managed in accordance with data protection legislation and school policies.
- Where available, additional security measures, such as encryption and multi-factor authentication, will be used to protect school accounts and information.

- **Responding to Online Safety Incidents and Concerns**

- All members of the community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting), cyberbullying and illegal content.
- All members of the community will be made aware of the availability of the Cyber Choices early intervention programme for individuals who are involved in cybercrime, or those who are gifted and talented and are at risk of becoming involved in cybercrime.
- All members of the community must respect confidentiality and the need to follow the official procedures for reporting concerns.
- Learners, parents and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.
- We require staff, parents, carers and learners to work in partnership to resolve online safety issues.
- After any investigations are completed, we will debrief, identify lessons learnt and implement any policy or curriculum changes as required.
- We will refer to the flow chart on responding to incidents, made available
- Where there is suspicion that illegal activity has taken place, we will follow the local safeguarding procedures which will include Police using 101, or 999 if there is immediate danger or risk of harm.
- If an incident or concern needs to be passed beyond our community (for example if other local settings are involved or the public may be at risk), the DSL will speak with Call Derbyshire/ Derbyshire Police first to ensure that potential investigations are not compromised.

10. Concerns about Learners Welfare

- The DSL (or deputy) will be informed of any online safety incidents involving safeguarding or child protection concerns.
    - The DSL (or deputy) will record these issues in line with our child protection policy.
- The DSL (or deputy) will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Derby and Derbyshire Safeguarding Children Partnership thresholds and procedures.
- We will inform parents and carers of online safety incidents or concerns involving their child, as and when required.

11. Procedures for Responding to Specific Online Incidents or Concerns

11.1 Online Sexual Violence and Sexual Harassment between Children

- Our school has accessed and understood "Sexual violence and sexual harassment between children in schools and colleges" guidance and part 5 of 'Keeping children safe in education'.
- Aston on Trent Primary School recognises that sexual violence and sexual harassment between children can take place online. Examples may include; non-consensual sharing of sexual images and videos, sexualised online bullying, online coercion and threats, unwanted sexual comments and messages on social media, and online sexual exploitation.
    - Full details of how we will respond to concerns relating to sexual violence and sexual harassment between children can be found within our child protection and anti-bullying policy.

- Aston on Trent Primary School recognises that internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities.
- Aston on Trent Primary School also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
  Aston on Trent Primary School will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment between children by implementing a range of age and ability appropriate educational methods as part of our PSHE and RSE curriculum. (see also anti-bullying/behaviour/acceptable use/images/equalities)
- We will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between children.
- We will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.
- If made aware of online sexual violence and sexual harassment, we will:
    - Immediately notify the DSL (or deputy) and act in accordance with our child protection and anti-bullying policies.
    - If content is contained on learners electronic devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
    - Provide the necessary safeguards and support for all learners involved, such as offering specific advice on blocking, reporting and removing online content, as well as providing appropriate counselling/pastoral support.
    - Implement appropriate sanctions in accordance with our behaviour policy
    - Inform parents and carers, if appropriate, about the incident and how it is being managed.
    - If appropriate, make a referral to partner agencies, such as Children's Social Work Service and/or the Police.

- If the concern involves children and young people at a different educational setting, work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community.
  - If a criminal offence has been committed, the DSL (or deputy) will discuss this with Derbyshire Police first to ensure that investigations are not compromised.
- Review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.

11.2 Youth Produced Sexual Imagery (nudes and semi-nudes).

- Aston on Trent Primary School recognises youth produced sexual imagery as a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy).
- We will follow current DfE guidance, including Sharing Nudes and Semi-Nudes: Advice for Education Settings Working with Children and Young People and Keeping Children Safe in Education.
- Aston on Trent Primary School will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of sharing nudes and semi-nudes by implementing preventative approaches, via a range of age and ability appropriate educational methods.
- We will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.
- We will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on site or using setting provided or personal equipment.
- We 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.
    - If it is deemed necessary, the image will only be viewed by the DSL (or deputy DSL) and their justification for viewing the image will be clearly documented.
  - Send, share, save or make copies of content suspected to be an indecent image of a child (i.e. youth produced sexual imagery) and will not allow or request learners to do so.

- If made aware of an incident involving the creation or distribution of youth produced sexual imagery, we will:
  - Act in accordance with our child protection policies and the relevant Derbyshire Safeguarding Children Partnership procedures.
  - Store the device securely.
    - If an indecent image has been taken or shared on our network or devices, we will act to block access to all users and isolate the image.
  - Carry out a risk assessment which considers any vulnerability of learners involved; including carrying out relevant checks with other agencies.
  - Inform parents and carers, if appropriate, about the incident and how it is being managed.
  - Make a referral to Children's Social Work Service and/or the Police, as deemed appropriate.

- Provide the necessary safeguards and support for learners, such as offering counselling or pastoral support.
- Implement appropriate sanctions in accordance with our behaviour policy but taking care not to further traumatise victims where possible.
- Images will only be deleted once the DSL has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation.
- Review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.

11.3 Online Child Sexual Abuse and Exploitation (including child criminal exploitation)

- Aston on Trent Primary School will ensure that all members of the community are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.
- Aston on Trent Primary School recognises online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL (or deputy).
- We will implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability appropriate education for learners, staff and parents/carers.
- We will ensure that all members of the community are aware of the support available regarding online child sexual abuse and exploitation (including criminal exploitation), both locally and nationally.
- We will ensure that the 'Click CEOP' report button is visible and available to learners and other members of our community.
- If made aware of incident involving online child sexual abuse and exploitation (including criminal exploitation), we will:
  - Act in accordance with our child protection policies and the relevant Derbyshire Safeguarding Children Partnership procedures.
  - If appropriate, store any devices involved securely.
  - Make a referral to Children's Social Work Service (if required/appropriate) and immediately inform Derbyshire police via 101, or 999 if a child is at immediate risk.
  - Carry out a risk assessment which considers the vulnerabilities, wishes, feelings and needs of the learner(s) involved, including undertaking relevant checks with other agencies where appropriate.
  - Inform parents/carers about the incident and how it is being managed.
  - Provide the necessary safeguards and support for learners, such as, offering counselling or pastoral support.
  - Review the handling of any incidents to ensure that best practice is implemented; leadership team will review and update any management procedures, where necessary.

    - Concerns identified through filtering and monitoring systems will be assessed and managed in accordance with safeguarding procedures.
- We will respond to concerns regarding online child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on our premises or using setting provided or personal equipment.
- Where possible, learners will be involved in decision making and if appropriate, will be empowered to report concerns such as via the Click CEOP report: www.ceop.police.uk/safety-centre/
- If we are unclear whether a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Derbyshire police by using 101.
- If made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the Derbyshire police using 101 unless immediate concerns and 999 will be used by the DSL (or deputy).
- If learners at other setting are believed to have been targeted, the DSL (or deputy) will seek support from Derbyshire Police first to ensure that potential investigations are not compromised.

11.4 Indecent Images of Children (IIOC)

- Aston on Trent Primary School will ensure that all members of the community are made aware of the possible consequences of accessing Child Sexual Abuse Material (CSAM).
- We will respond to concerns regarding CSAM on our equipment and/or personal equipment, even if access took place off site.
- We will seek to prevent accidental access to CSAM by using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software.
- If we are unclear if a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Derbyshire Police using 101.

- If made aware of CSAM, we will:
    - Act in accordance with our child protection policy and the relevant Derby City & Derbyshire Safeguarding Children Partnership Safeguarding procedures.
    - Store any devices involved securely.
    - Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), Derbyshire police or the LADO.

- If made aware that a member of staff or a learner has been inadvertently exposed to indecent images of children, we will:
    - Ensure that the DSL (or deputy) is informed.
    - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
    - Do not forward, copy, print, save or further distribute any suspected indecent images.
    - Follow Police, Children's Social Care or other agency advice regarding the retention or deletion of any material.

- Report concerns, as appropriate to parents and carers.

- If made aware that indecent images of children have been found on the setting provided devices, we will:
  - Ensure that the DSL (or deputy) is informed.
  - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
  - Ensure that suspected indecent images are not copied, printed, shared, forwarded, downloaded or further distributed.
  - Follow the advice of the Police and other relevant agencies regarding the retention, deletion or preservation of any suspected indecent images or related material.
  - Only retain copies of images where specifically directed to do so by the Police and ensure that any retained material is stored securely with restricted access.
  - Report concerns, as appropriate to parents and carers.

- If made aware that a member of staff is in possession of indecent images of children on setting provided devices, we will:
  - Ensure that the *headteacher* is informed in line with our managing allegations against staff policy immediately and without any delay.
  - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with our managing allegations against staff policy.
  - Quarantine any devices until police advice has been sought.

11.5 Cyberbullying

- Cyberbullying, along with all other forms of bullying, will not be tolerated at Aston on Trent Primary School.
- Full details of how we will respond to cyberbullying are set out in our anti-bullying policy.

11.6 Online Hate

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at Aston on Trent Primary School and will be responded to in line with existing policies, including anti-bullying and behaviour.
- All members of the community will be advised to report online hate in accordance with relevant policies and procedures.
- Online hate may include content or behaviour that targets individuals or groups based on protected characteristics, including race, religion, disability, sex, sexual orientation, gender reassignment or other protected characteristics.
- The Police will be contacted if a criminal offence is suspected.
- If we are unclear how to respond, or whether a criminal offence may have been committed, the DSL (or Deputy DSL) will seek advice from Derbyshire Police and other appropriate agencies (https://www.saferderbyshire.gov.uk/home.aspx).
- Concerns relating to online hate will be reviewed to determine whether they also raise safeguarding concerns, including radicalisation, extremism, harassment or hate crime.

11.7 Online Radicalisation and Extremism

- We will take all reasonable precautions to ensure that learners and staff are safe from terrorist and extremist material when accessing the internet on site. (See the Extremism and Radicalisation Policy)
- If we are concerned that a child or parent/carer may be at risk of radicalisation online, the DSL (or deputy) will be informed immediately, and action will be taken in line with our child protection policy and Derbyshire prevent pathway which may include a referral into Channel.
- If we are concerned that member of staff may be at risk of radicalisation online, the *headteacher* will be informed immediately, and action will be taken in line with the child protection and allegations policies.

11.8 Cybercrime

- Cybercrime incidents and offences will be responded to in line with our existing behaviour policies.
- We will respond to concerns that our students are involved, or at risk of becoming involved, in cybercrime, even if it takes place off site.
- We will make a Cyber Choices referral for early intervention, as per the Cyber Choices toolkit.
- If we are concerned that a child is being exploited as a result of their technical skills, we will follow the Children at Risk of Exploitation (CRE) procedure and the CRE Risk Assessment Toolkit

12. Useful Links for Educational Settings

Support and Guidance for Educational Settings

Derby City & Derbyshire Safeguarding Children Partnership online procedures DDCSP:

https://www.ddscp.org.uk/staff-and-volunteers/policies-and-procedures/

Derbyshire Police:

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

LADO

- By referral into Professional.Allegations@derbyshire.gov.uk
- Form found here http://derbyshirescbs.proceduresonline.com/docs_library.html

Call Derbyshire (Starting Point)

- Immediate risk of harm phone 01629 533190
- For all other referrals complete an online form https://www.derbyshire.gov.uk/social-health/children-and-families/support-for-families/starting-point-referral-form/starting-point-request-for-support-form.aspx
- For professional advice phone 10629 535353

National Links and Resources for Educational Settings

- CEOP:
  - www.thinkuknow.co.uk
  - www.ceop.police.uk
- Childnet: www.childnet.com
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety
  - ChildLine: www.childline.org.uk
  - Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk
  - Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
- 360 Safe Self-Review tool for schools: www.360safe.org.uk

National Links and Resources for Parents/Carers

- Action Fraud: www.actionfraud.police.uk

- CEOP:
  - www.thinkuknow.co.uk
  - www.ceop.police.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
- NSPCC: www.nspcc.org.uk/onlinesafety
  - ChildLine: www.childline.org.uk
  - Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk