Abbots Farm Junior School

Online Safety Policy



Key Details

Designated Safeguarding Lead: Gemma Webb - Headteacher

Designated Online Safety lead: Vinaya Neel - Computing Lead

Deputy DSLs: Adam Corbett - Deputy Headteacher, Lauren Watson-Tate – Assistant Headteacher/SENCO

Named Governor with lead responsibility: Lisa Bell

Date written: January 2020

Date of last review: November 2026

Date of next review: November 2027

This policy will be reviewed at least annually. It will also be revised following any

Contents

	Page no
1. Policy Aims	4
2. Policy Scope	4
2.2 Links with other policies and practices	5
3. Monitoring and Review	5
4. Roles and Responsibilities	5
4.1 The leadership and management team	5
4.2 The Designated Safeguarding Lead	6
4.3 Members of staff	7
4.4 Staff who manage the technical environment	7
4.5 Pupils	7
4.6 Parents	8
5. Education and Engagement Approaches	8
5.1 Education and engagement with pupils	8
5.2 Vulnerable Pupils	9
5.3 Training and engagement with staff	9
5.4 Awareness and engagement with parents	9
6. Reducing Online Risks	10
7. Safer Use of Technology	10
7.1 Classroom Use	10
7.2 Managing Internet Access	11
7.3 Filtering and Monitoring	11
7.4 Managing Personal Data Online	12
7.5 Security and Management of Information Systems	12
7.6 Managing the Safety of the Website	13
7.7 Publishing Images and Videos Online	13
7.8 Managing Email	13
8. Responding to Online Safety Incidents and Concerns	13
8.1 Concerns about Pupil Welfare	13
8.2 Staff Misuse	14
9. Procedures for Responding to Specific Online Incidents or Concerns	14
9.1 Online Sexual Violence and Sexual Harassment between Children	14
9.2 Youth Produced Sexual Imagery or “Sexting”	15
9.3 Online Child Sexual Abuse and Exploitation	16
9.4 Indecent Images of Children (IIOC)	17
9.5 Cyberbullying	18
9.6 Online Hate	18
9.7 Online Radicalisation and Extremism	19
10. Useful Links for Educational Settings	19

Abbots Farm Junior School Online Safety Policy

1. Policy Aims

This online safety policy has been written by Abbots Farm Junior School involving staff, pupils and parents/carers, building on the Kent County Council/The Education People online safety policy template, with specialist advice and input as required.

It takes into account the DfE statutory guidance 'Keeping Children Safe in Education', 'Working Together to Safeguard Children' and the Warwickshire Safeguarding Children Partnership guidance.

The purpose of Abbots Farm Junior School's online safety policy is to:

- Safeguard and protect all members of the Abbots Farm Junior School community online.
- Identify approaches to educate and raise awareness of online safety throughout the community.
- Enable all staff to work safely and responsibly, 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.

Abbots Farm Junior School identifies that the issues classified within online safety are considerable, but can be broadly categorised into three 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.

Online safety expectations apply not only to devices in school but also to:

- smart watches
- wearable technology
- AI-enabled devices
- personal internet-connected devices

2. Policy Scope

- Abbots Farm Junior School believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all pupils and staff are protected from potential harm online.
- Abbots Farm Junior School identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life.
- Abbots Farm Junior School believes that pupils 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 pupils, parents and carers.
- This policy applies to all access to the internet and use of technology, including personal devices, or where pupils, staff or other individuals have been provided with setting issued devices for use off-site, such as a work laptops, tablets or mobile phones.

2.2 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)
- Code of conduct (staff behaviour) policy
- Child protection policy
- Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE), and Relationships and Sex Education (RSE)
- Data protection
- GDPR
- Use of mobile phones and personal devices policy
- Staff/Governor use of social media policy
- Relationships and behaviour policy

3. Monitoring and Review

- Technology in this area evolves and changes rapidly. Abbots Farm Junior 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 Deputy Headteacher will be informed of online safety concerns, as appropriate.
- Online safety is reported to governors termly via the Headteacher's safeguarding report. The named governor for safeguarding will review online safety practice and incidents, including outcomes annually.
- Any issues identified via monitoring will be incorporated into our action planning.

4. Roles and Responsibilities

- The Designated Safeguarding Lead (DSL) (Gemma Webb, Headteacher) has overall responsibility for online safety but the Online Safety Lead (Vinaya Neel, Computing Lead) takes the lead in following up online safety incidents initially.
- Abbots Farm Junior 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 acceptable 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 pupils 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 there are robust reporting channels for the community to access regarding online safety concerns, including internal, local and national support.

- Audit and evaluate online safety practice to identify strengths and areas for improvement.

4.2 The Designated Online Safety Lead 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 DSLs to ensure online safety is recognised as part of the setting's 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 pupils safe online.
- Access regular and appropriate training and support to ensure they recognise the additional risks that pupils 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 with the governor with a lead responsibility for safeguarding

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, use of mobile phones and personal devices policy, the use of social media 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.

4.4 It is the responsibility of staff managing the technical environment to:

- Provide technical support and perspective to the DSL, online safety lead and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Implement appropriate security measures including Encrypted wi-fi, Encrypted devices, Password protected devices, Firewalls and 'Policy Central' Filtering System as directed by the leadership team 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 and monitoring systems are applied and updated on a regular basis through Warwickshire Education Services (WES); responsibility for its implementation is shared with the leadership team
- Ensure the DSL (and/or deputy) are alerted to any safeguarding concerns raised through our filtering and monitoring systems, to enable them to take appropriate safeguarding action if/when required.

4.5 It is the responsibility of pupils (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.

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.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

5. Education and Engagement Approaches

5.1 Education and engagement with pupils

- The setting will establish and embed a progressive online safety curriculum to raise awareness and promote safe and responsible internet use amongst pupils 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.
    - Reinforcing online safety messages whenever technology or the internet is in use.
    - Educating pupils in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.

- Teaching pupils to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

- The setting will support pupils 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 pupils that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
  - Rewarding positive use of technology.
  - Teaching online safety and media literacy lessons which revisit key messages every year, to include:
    - fake news
    - misinformation
    - disinformation
    - manipulated content
    - digital footprints
    - online reputation
    - permanent nature of online content

  - Seeking pupil 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 Pupils

- Abbots Farm Junior School recognises that some pupils 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) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.
- Abbots Farm Junior School will ensure that differentiated and ability-appropriate online safety education, access and support is provided to vulnerable pupils.
- When implementing an appropriate online safety policy and curriculum Abbots Farm Junior School will seek input from specialist staff as appropriate, including the SENCO, Child in Care Designated Teacher and any necessary external support.

5.3 Training and engagement with staff

We will:

- Provide and discuss the online safety policy and procedures and other linked policies with all members of staff as part of induction.
- Provide up-to-date and appropriate online safety training for all staff on a regular basis, with at least annual updates.
  - This will cover the potential risks posed to pupils (Content, Contact and Conduct) as well as our professional practice expectations.
- 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.

- 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 pupils.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting pupils, colleagues or other members of the community.

5.4 Awareness and engagement with parents and carers

- Abbots Farm Junior 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 information and guidance on online safety in a variety of formats.
    - Drawing their attention to the online safety policy and expectations in newsletters, letters, our prospectus and on our website.
    - Requesting that they read online safety information our acceptable use policies as part of joining our community and discuss the implications with their children.

6. Reducing Online Risks

- Abbots Farm Junior 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 for educational benefit and undertake appropriate risk assessments before use in the setting is permitted.
    - 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 but we will ensure that children are always reminded to 'close it and report it' and this message will be displayed on posters throughout school.
- 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

- Abbots Farm Junior School uses a wide range of technology. This includes access to:
    - Laptops and iPads
    - Internet which may include search engines and educational websites
    - The WeLearn Learning Platform including Email

    - Seesaw
- All Abbots Farm Junior School owned devices will be used in accordance with our acceptable use policies and with appropriate safety and security measures in place.
    - Zulu Desk is used as the mobile device management software in school and is only accessed by SLT and our ICT support team at Launch
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- Members of staff will use and promote the following age-appropriate search tools where possible and teach and monitor safe searching habits.
    - https://www.kiddle.co
    - https://swiggle.org.uk
    - https://www.dkfindout.com/uk/ (great for subject specific information such as animals)
    - https://www.bbc.co.uk/cbbc/search (searches all BBC resources)
- Supervision of pupils will be appropriate to their age and ability.
    - **Key Stage 2**
        - Pupils will use age-appropriate search engines and online tools.
        - Pupils will be directed by the teacher to online materials and resources which support the learning outcomes planned for the pupils' age and ability.

7.2 Artificial Intelligence (AI)

- Abbots Farm Junior School recognises that artificial intelligence (AI) technologies, including generative AI tools, present both educational opportunities and safeguarding risks. The school will ensure that staff and pupils receive age-appropriate education regarding the safe, responsible and ethical use of AI technologies, including the risks associated with misinformation, deepfakes, online scams, privacy and inappropriate content.

7.3 Cyber Security and Digital Resilience

Abbots Farm Junior School recognises that cyber security is an essential part of safeguarding, business continuity and data protection. Cyber incidents can affect the welfare of children, compromise sensitive information and disrupt teaching and learning.

The school will:

- Maintain appropriate security measures to protect systems, devices, networks and data from unauthorised access, loss, damage or misuse.
- Ensure that anti-virus, filtering, monitoring and security updates are applied to school devices and systems in a timely manner.
- Work with Warwickshire Education Services (WES) and other technical support providers to identify and manage cyber security risks.
- Promote strong password practices and ensure staff understand their responsibilities for keeping login credentials secure.
- Provide staff with regular training and reminders about cyber security, including recognising phishing emails, scams, malicious links and social engineering attempts.
- Ensure that suspected cyber incidents, data breaches or security concerns are reported promptly to the Headteacher, DSL and technical support providers as appropriate.
- Maintain appropriate backup and recovery arrangements to support business continuity in the event of a cyber incident.

- Review cyber security risks regularly as part of the school's wider safeguarding, risk management and data protection arrangements.

All staff will:

- Remain vigilant to suspicious emails, messages, websites or requests for information.
- Verify unusual requests for financial, personal or sensitive information before responding.
- Report suspected phishing emails, malware, data breaches or security concerns immediately.
- Lock devices when unattended and store school information securely.
- Only use approved systems and software for storing and processing school information.

Pupils will be taught, at an age-appropriate level, to:

- Create and manage secure passwords.
- Recognise scams, phishing and fraudulent online activity.
- Understand how to protect personal information online.
- Report anything online which makes them feel unsafe, worried or uncomfortable.
- Develop an understanding that not all online content, messages, images and videos are trustworthy.

7.4 Managing Internet Access

- We will maintain a written record of users who are granted access to our devices and systems.
- All staff, pupils and visitors will read and sign an acceptable use policy before being given access to our computer system, IT resources or internet.

7.5 Filtering and Monitoring

7.5.1 Decision Making

- Abbots Farm Junior School governors and leaders have ensured that our setting has age and ability appropriate filtering and monitoring in place, to limit pupils' 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 pupils; effective classroom management and regular education about safe and responsible use is essential.

7.5.2 Filtering

- Education broadband connectivity is provided through BT Openreach via Warwickshire County Council
- We use a monitored firewall provided by Warwickshire County Council which blocks sites which can be categorised as: pornography, racial hatred, extremism, gaming, sponsored adverts and sites of an illegal nature.

- We also use Policy Central, which is a keystroke recognition programme provided via Warwickshire County Council that gives instant updates to school on any inappropriate language typed into school laptops.
- If pupils discover unsuitable sites:
    - The child must close the lid on the laptop/iPad and 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 Online Safety 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.
- Any material believed to be illegal will be reported immediately to the appropriate agencies, such as the IWF, Warwickshire Police or CEOP.

7.5.3 Monitoring

- We will appropriately monitor internet use on all Abbots Farm Junior School owned or provided internet enabled devices. This is achieved by:
    - Supervision of children on all internet-enabled devices alongside the use of Policy Central Filtering and the keystroke monitoring programme.
- If a concern is identified via monitoring approaches, the DSL for online safety or a deputy will respond in line with the relevant school policies (e.g. relationship and behaviour policy/child protection policy)
- All users will be informed that use of our systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

Governors receive regular assurance that filtering and monitoring systems are effective and that safeguarding concerns identified through monitoring are reviewed and acted upon appropriately.

7.6 Managing Personal Data Online

- Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations and Data Protection legislation.
    - Full information can be found in our Information Security and Data Protection policies.

7.7 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 checking files held on our network.
    - The appropriate use of user logins and passwords to access our network.
        - Specific user logins and passwords will be enforced for all pupils
    - All users are expected to log off or lock their screens/devices if systems are unattended.
    - Further information about technical environment safety and security can be found in:
        - acceptable use policy

- information security policy
- staff handbook

7.7.1 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 private.
- All pupils are provided with their own unique username and private passwords to access our systems; pupils are responsible for keeping their password private.
- We require all users to:
    - Use strong passwords for access into our system.
    - Always keep their password private; users must not share it with others or leave it where others can find it.
    - Not to login as another user at any time.

7.8 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 pupils' 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.

7.9 Publishing Images and Videos Online

- We will ensure that all images and videos shared online are used in accordance with the associated polices, including (but not limited to) the: cameras and image use, data security, acceptable use policies, codes of conduct/behaviour, social media and use of personal devices and mobile phones.

7.10 Managing Emails

- 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 (WeLearn to WeLearn emails are automatically encrypted)
    - School 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 the headteacher if they receive offensive communication, and this will be recorded in our safeguarding files/records.
- The use of personal email addresses by staff for any official setting business is not permitted.
    - All members of staff are provided with an email address to use for all official communication.

- Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff, pupils and parents.

8. 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 must respect confidentiality and the need to follow the official procedures for reporting concerns.
    - Pupils, 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 pupils 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.
- If we are unsure how to proceed with an incident or concern, the DSL (or deputy) will seek advice from the Education Safeguarding Service.
- Where there is suspicion that illegal activity has taken place, we will contact Warwickshire Education Safeguarding Service or Warwickshire 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 headteacher will speak with Warwickshire Police and/or the Education Safeguarding Service first to ensure that potential investigations are not compromised.

8.1 Concerns about Pupils 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 Warwickshire 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.

8.2 Staff Misuse

- Any complaint about staff misuse will be referred to the headteacher, in accordance with the allegations policy.
- Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- Appropriate action will be taken in accordance with our staff behaviour policy/code of conduct.

9. Procedures for Responding to Specific Online Incidents or Concerns

9.1 Online Sexual Violence and Sexual Harassment between Children

- Our setting 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'.
- Abbots Farm Junior 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.
- Abbots Farm Junior 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.
- Abbots Farm Junior School also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
- Abbots Farm Junior 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.
- 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 pupils electronic devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
    - Provide the necessary safeguards and support for all pupils 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 relationships and 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 Warwickshire 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.

9.2 Youth Produced Sexual Imagery ("Sexting")

- Abbots Farm Junior School recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy).
- Abbots Farm Junior School will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of 'sexting' by implementing preventative approaches, via a range of age and ability appropriate educational methods.

- 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 pupils 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 Warwickshire Safeguarding Child Board's 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 pupils 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, if deemed appropriate
    - Provide the necessary safeguards and support for pupils, such as offering counselling or pastoral support.
    - Implement appropriate sanctions in accordance with our relationships and behaviour policy but taking care not to further traumatise victims where possible.
    - Consider the deletion of images in accordance with relevant, current guidance.
        - 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.

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

- Abbots Farm Junior 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.
- Abbots Farm Junior 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 pupils, 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 used to report online child sexual abuse is visible and available to pupils and other members of our community.
- If made aware of an incident involving online child sexual abuse and exploitation (including criminal exploitation), we will:

- Act in accordance with our child protection policies and the relevant Kent Safeguarding Child Board's procedures.
- If appropriate, store any devices involved securely.
- Make a referral to Children's Social Work Service (if required/appropriate) and immediately inform Warwickshire police via 101, or 999 if a child is at immediate risk.
- Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).
- Inform parents/carers about the incident and how it is being managed.
- Provide the necessary safeguards and support for pupils, 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.

- 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, pupils 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 Education Safeguarding Service and/or Warwickshire Police.
- If made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the relevant agencies by the DSL (or deputy).
- If pupils at other setting are believed to have been targeted, the DSL (or deputy) will seek support from the Police and/or the Education Safeguarding Service first to ensure that potential investigations are not compromised.

9.4 Indecent Images of Children (IIOC)

- Abbots Farm Junior School will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).
- We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.
- We will seek to prevent accidental access to IIOC 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 Police and/or the Education Safeguarding Service.
- If made aware of IIOC, we will:
  - Act in accordance with our child protection policy and the relevant Warwickshire Safeguarding Child Boards procedures.
  - Store any devices involved securely.
  - Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), Warwickshire police.

- If made aware that a member of staff or a pupil 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 .

- Ensure that any copies that exist of the image, for example in emails, are deleted.
- 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 any copies that exist of the image, for example in emails, are deleted.
  - Inform the police via 101 (999 if there is an immediate risk of harm) and Children's Social Work Service (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.
  - 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.
  - 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.

9.5 Cyberbullying

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

9.6 Online Hate

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at Abbots Farm Junior 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.
- The Police will be contacted if a criminal offence is suspected.
- If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL (or deputy) will obtain advice through the Education Safeguarding Service and/or Warwickshire Police.

9.7 Online Radicalisation and Extremism

- We will take all reasonable precautions to ensure that pupils and staff are safe from terrorist and extremist material when accessing the internet on site.
- 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.
- 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.

10. Useful Links for Educational Settings

Warwickshire Support and Guidance for Educational Settings

Education Safeguarding Service:

- There is now a central point of contact for all staff in the Education Safeguarding Team. They can be called on 01926 743000 or emailed at educationsafeguarding@warwickshire.gov.uk

Children and Families Front Door

- For any significant safeguarding concerns that arise from an online safety concern, call 01926 414144

Warwickshire Police:

https://www.warwickshire.police.uk/police-forces/warwickshire-police/areas/warwickshire-police/campaigns/campaigns/2019/be-cyber-smart

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

Other:

- ICTDS – Warwickshire ICT Development Services https://www.ictds.org/online-safety

National Links and Resources for Educational Settings

- National Online Safety: https://nationalonlinesafety.com
- 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

- National Online Safety: https://nationalonlinesafety.com
- 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