Dovecotes Primary School
Online Safety Policy

Digital Safeguarding
(including Social Media)

Key Details

Designated Safeguarding Lead (DSL): Tracy Challenor (Headteacher)

Deputy DSLs (DDSLs): Laura Jones (Deputy Head), Lesley Hehir (Learning Mentor)

Online Safety Lead (OSL): Tracy Challenor

Deputy Online Safety Lead (OSL): Lindsey Gould

Named Governor with lead responsibility: Tim Wakefield, Chair of Governors

Date written: September 2022 (updated Feb 23)

Date agreed and ratified by Governing Body: March 23

Date of next review: by September 2023

This policy will be reviewed **at least** annually. It will also be revised following any concerns and/or updates to national and local guidance or procedures.

Contents

Dovecotes Primary School Online Safety Policy

1. Policy aims

- This online safety policy has been written by Dovecotes Primary School, involving staff, learners and parents/carers, building on The Education People online safety policy template, with specialist advice and input from Online Behaviours Ltd.
- It takes into account the DfE statutory guidance 'Keeping Children Safe in Education' 2022, Early Years and Foundation Stage 2017 'Working Together to Safeguard Children' and DfE 'Safeguarding and remote education during coronavirus (COVID-19)'
- This policy should also be read in conjunction with Ofsted's 'Review of sexual abuse in schools and colleges' and UKCIS Sharing nudes and semi-nudes: advice for education settings working with children and young people and DfE Behaviour in Schools 2022.
- Dovecotes Primary School is currently operating in response to coronavirus (Covid-19); our safeguarding principles in accordance with 'Keeping Children Safe in Education' (KCSIE) 2022 and related guidance, however, remain the same.
    - Where children are asked to learn online at home in response to a full or partial closure, we will follow expectations as set out within the Safeguarding & Child Protection Policy and in line with DfE Guidance, 'Safeguarding and remote education during coronavirus (COVID-19)' 2020.
- The purpose of this online safety policy is to:
    - safeguard and promote the welfare of all members of the Dovecotes Primary School community online.
    - identify approaches to educate and raise awareness of online safety throughout our 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 follow when responding to online safety concerns.
- Dovecotes Primary 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.
    - **Commercial:** risks such as online gambling, access to inappropriate advertising, phishing, in-game purchasing and/or financial scams.

2. Policy scope

- Dovecotes Primary School recognises that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all learners/staff are protected from potential harm online.
- Dovecotes 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 which present positive and exciting opportunities, as well as challenges and risks.
- Dovecotes Primary School will empower our learners to acquire the knowledge needed to use the internet and technology in a safe, considered and respectful way, and develop their resilience so they can manage and respond to online risks.
- This policy applies to all staff, including the governing body, senior leadership team (SLT), teachers, support staff, office and site 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 and parents and carers.
- This policy applies to all access to the internet and use of technology, including mobile technology, or where learners, staff or other individuals have been provided with setting issued devices for use, both on and off-site.

2.2 Links with other policies and practices

- This policy links with other policies, practices and action plans, including but not limited to:
    - Anti-bullying policy;
    - Acceptable Use Policies (AUP) and/or the Code of conduct and Staff Device Agreement;
    - Behaviour policy;
    - Inclusion and discipline policy;
    - Child protection policy & Safeguarding;
    - Curriculum policies/overviews, including: Computing, Personal Social and Health Education (PSHE), Citizenship and Relationships and Sex Education (RSE);
    - Data Protection/Security;
    - Mobile phone policy;
    - Use of pupil images policy;
    - Searching, screening and confiscation documentation.

3. Monitoring and review

- Technology evolves and changes rapidly; as such Dovecotes Primary School will review this policy at least annually. The policy will be revised following any national or local policy updates, any local child protection concerns and/or changes to our 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 DSL/ Online Safety Lead (Headteacher, Tracy Challenor), DDSLs (Laura Jones and Lesley Hehir) and Deputy Online Safety Lead (Lindsey Gould) will be informed of online safety concerns, as appropriate.
- The named governor for safeguarding (Tim Wakefield) will report on online safety practice and incidents, including outcomes, on a regular basis to the wider governing body.

- Any issues identified via monitoring policy compliance will be incorporated into action plans.

4. Roles and Responsibilities

- The Designated Safeguarding Lead (DSL, Headteacher – Tracy Challenor) is recognised as holding overall lead responsibility for online safety, in line with KCSIE 2022.
- The Deputy Designated Safeguarding Leads (DDSLs, Laura Jones – Deputy Head; Lesley Hehir – Learning Mentor) together with the Online Safety Lead (Tracy Challenor), Deputy Online Safety Lead (Lindsey Gould) will support the DSL in this role, ensuring everything is passed onto/via the DSL.
- Dovecotes Primary School recognises that all members of the community, including but not limited to care givers (school staff, parents and carers) have important roles and responsibilities to play with regards to online safety.

4.1 The Senior Leadership Team (SLT) will:

- Create a whole setting culture that incorporates online safety throughout all elements of Dovecotes Primary School life.
- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Implement appropriate and up-to-date policies regarding online safety which addresses the acceptable use of technology, child-on-child abuse, social media use and mobile technology.
- Work with technical staff and IT support to ensure that suitable and appropriate filtering and monitoring systems are in place.
- Support the DSL and any deputies by ensuring they have enough time and resources to carry out their responsibilities.
- Ensure robust reporting channels are in place for the whole community to access regarding online safety concerns (use of both paper based recording and CPOMs as well as SENSO).
- Undertake appropriate risk assessments regarding the safe use of technology on site.
- Audit and evaluate online safety practice to identify strengths and areas for improvement.
- Ensure that staff, learners and parents/carers are proactively engaged in activities which promote online safety.
- Support staff to ensure that online safety is embedded within a progressive whole setting curriculum which enables all learners to develop an appropriate understanding of online safety.

4.2 The Designated Safeguarding Lead (DSL) will:

- Act as a named point of contact within the setting on all online safeguarding issues.
- Liaise with other members of staff, such as DDSLs, Online Safety lead, IT technicians, network managers and the SENCO on matters of online safety.
- Ensure appropriate referrals are made to relevant external partner agencies, as appropriate.

- Work alongside DDSLs to ensure online safety is recognised as part of the setting's safeguarding responsibilities, and that a coordinated whole school approach is implemented.
- Access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant and up-to-date knowledge 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.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and child protection training.
- 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 setting's safeguarding recording mechanisms.
- Monitor online safety incidents to identify gaps and trends and use this data to update the education response and school's policies and procedures.
- Report online safety concerns, as appropriate, to the SLT and Governing Body.
- Work with the SLT to review and update online safety policies regularly (at least annually).
- Meet regularly (at least termly) with the governor with a lead responsibility for safeguarding and online safety.
- Meet regularly (at least termly) with the Online Safety Group (Digital Leaders) to ensure staff, pupils and/or parents are updated and informed.

4.25 It is the responsibility of curriculum leads to:

- Work with the Online Safety Lead to develop a planned and co-ordinated online safety education programme, which will be provided through:
    - PSHE and RSE programme of Jigsaw
    - A mapped cross-curricular programme, which is in development by the OSL
    - Assemblies and pastoral care
    - Relevant national initiatives including Safer Internet Day and Anti-bullying week.

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

- Contribute to the development and implementation of our online safety policies.
- Read and adhere to our online safety policy and acceptable use of technology policies.
- Take responsibility for the security of IT systems and the electronic data they use or have access to.
- Model good practice when using technology with learners.
- Maintain a professional level of conduct in their personal use of technology, both on/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 learners in their care.
- Identify online safety concerns and take appropriate action by following the school safeguarding policies and procedures.
- Know when and how to escalate online safety issues, including reporting to the DSL and/or Online Safety Lead and signposting learners and parents/carers 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/perspective to the DSL, Online Safety Lead and SLT, especially in the development and implementation of appropriate online safety policies and procedures.
- Implement appropriate security measures including the use of filtering and monitoring as directed by the SLT to ensure that the settings IT infrastructure is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensure that our filtering policy and monitoring systems and approaches are applied and updated on a regular basis; responsibility for its implementation is shared with the SLT.
- Ensure appropriate technical support and access to our filtering and monitoring systems is given to the DSL and/or deputies to enable them to take appropriate safeguarding action 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/ability appropriate online safety education.
- Contribute to the development of online safety policies.
- Read and adhere to the acceptable use of technology and behaviour policies.
- Respect the feelings and rights of others, on and offline.
- Take an appropriate level of responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if they are concerned about anything, they or others experience online.

4.6 It is the responsibility of parents and carers to:

- Read our acceptable use of technology policies and encourage 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 and abide by the home-school agreement and acceptable use of technology policies.

- Seek help and support from the school and/or other appropriate agencies, if they or their child encounter online issues.
- Contribute to the development of our online safety policies.
- Use our systems, such as learning platforms, website and other IT resources, safely and appropriately.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by the new and emerging technologies that their children access and use at home.

5. Education and engagement approaches

5.1 Education and engagement with learners

- The setting will establish and embed a whole school culture and will raise awareness and promote safe and responsible internet use amongst learners by:
    - ensuring our curriculum and whole school approach is developed in line with the UK Council for Internet Safety (UKCIS)) 'Education for a Connected World Framework 2020' and DfE 'Teaching online safety in school' guidance.
    - ensuring online safety is addressed through whole school approaches and specifically celebrated days as well as through Computing and PSHE programmes of study in Relationships (and Sex) Education, Health Education and Citizenship.
    - reinforcing online safety principles in other curriculum subjects as appropriate, and whenever technology or the internet is used on site.
    - creating a safe environment in which all learners feel comfortable to say what they feel, without fear of getting into trouble and/or being judged for talking about something which happened to them online.
    - involving the DSL (or DDSL) and/or Online Safety Lead as part of planning for online safety lessons or activities, so they can advise on any known safeguarding cases, and ensure support is in place for any learners who may be impacted by the content.
    - making informed decisions to ensure that any educational resources used are appropriate for our learners.
    - using external visitors, where appropriate, to complement and support our internal online safety education approaches.
    - providing online safety education as part of the transition programme across the key stages and/or when moving between establishments.
    - rewarding positive use of technology including with Achievement awards/assembly.

- Dovecotes Primary School will support learners to understand and follow our 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 network and internet use will be monitored for safety and security purposes, and in accordance with legislation.

    - seeking learner voice when writing and developing online safety policies and practices, including curriculum development and implementation.

- Dovecotes Primary School will ensure learners develop the underpinning knowledge and behaviours needed to navigate the online world safely, in a way that suits their age/ability by:
    - ensuring age-appropriate education regarding safe and responsible use precedes internet access.
    - teaching learners to evaluate what they see online and recognise techniques used for persuasion, so they can make effective judgements about if what they see is true, valid or acceptable.
    - educating them in the effective use of the internet to research, including the skills of knowledge location, retrieval and evaluation.
    - enabling them to understand what acceptable and unacceptable online behaviour looks like.
    - preparing them to identify possible online risks and make informed decisions about how to act and respond.
    - ensuring they know how and when to seek support if they are concerned or upset by something they see or experience online.

5.2 Vulnerable Learners

- Dovecotes Primary School recognises that any learner can be vulnerable online, and vulnerability can fluctuate depending on their age, developmental stage and personal circumstances. However, there are some learners, for example looked after children and those with special educational needs, who may be more susceptible or may have less support in staying safe online.
- Dovecotes Primary School will ensure that differentiated and appropriate online safety education, access and support is provided to vulnerable learners.
- Staff at Dovecotes Primary School will seek input from specialist staff as appropriate, including the DSL, SENCO, Child in Care designated representative (learning mentor/DDSL) to ensure that the policy and curriculum is appropriate to our community's needs.

5.3 Training and engagement with staff

- We will:
    - provide and discuss the online safety policy, AUPs and procedures with all members of staff as part of induction.
    - provide up-to-date and appropriate online safety training for all staff which is integrated, aligned and considered as part of our overarching safeguarding approach but delivered separately to the existing annual safeguarding/child protection training.
    - Staff training covers the potential risks posed to learners (content, contact, conduct and commerce) as well as our professional practice expectations.

- build on existing expertise by providing opportunities for staff to contribute to and shape our online safety approaches, including curriculum, 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, including personal use of social media, can have an impact on their professional role and reputation.
- highlight useful educational resources and tools which staff could use with learners.
- ensure all members of staff are aware of the procedures to follow regarding online safety concerns involving learners, colleagues or other members of the community.

5.4 Awareness and engagement with parents and carers

- Dovecotes 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 information and guidance on online safety in a variety of formats, including through the school website, during parents' evening and transition/welcome sessions.
  - drawing their attention to our online safety policy and expectations in our newsletters and other external communication (such as letters and the messaging service) as well as in our prospectus and on our website.
  - requesting parents and carers read online safety information as part of joining our community, for example, through the website and home school agreement.
  - requiring them to read our acceptable use policies and discuss the implications with their children.

6. Reducing Online Risks

- Dovecotes 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 for educational benefit and undertake appropriate risk assessments before their use in the school is permitted.
  - ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that access is appropriate.
  - recognise that due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via our systems or devices and as such identify clear procedures to follow if breaches or concerns arise.
- 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. This is clearly outlined in our AUPs and highlighted through a variety of education and training approaches.

7. Safer Use of Technology

7.1 Classroom use

- Dovecotes Primary School uses a wide range of technology. This includes access to:
  - Computers, laptops, tablets and other digital devices;
  - Internet, which may include search engines and educational websites;
  - Teams (recently implemented through school as a priority for Remote Learning);
  - Account access to specific sites, including Active Learn and Times Tables Rock Stars;
  - 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 of technology policies and with appropriate safety and security measures in place.
  - iPads are all password protected and content is wiped at least annually but often termly with remote locking and wiping managed by technicians;
  - Laptops all have Windows10 with Bitlocker and are encrypted.
- Members of staff will always evaluate websites, (particularly YouTube), tools and apps fully before use in the classroom or recommending for use at home.
  - The use of Safeyoutube.net to be used to share youtube videos without other content.
- The setting will use appropriate search tools as identified following an informed risk assessment.
  - Differentiated search engines are to be used for different age groups: **SWGfL Swiggle** to be set as a default home page and used as the main search engine for children up to year 4; years 4, 5 and 6 to use Google in line with the Online Safety framework with particular vigilance through safe searches, history checks and SENSO monitoring.
- 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 internet access and technology use will be appropriate to learners age/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' ages and abilities.
  - **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' ages and abilities.

7.2 Managing internet access

- We will maintain a written record of users who are granted access to our devices and systems, including Wi-Fi.

- All staff, learners and visitors will read and agree an acceptable use policy before being given access to our computer system, IT resources or the internet.

7.3 Filtering and monitoring

7.3.1 Decision making

- Dovecotes Primary School governors and leaders have ensured that our school has age and ability appropriate filtering and monitoring in place to limit learner's exposure to online risks.
- 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.
- The governors and leaders are mindful to ensure that "over blocking" does not unreasonably restrict access to educational activities and safeguarding materials.
- 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 Appropriate filtering

- Dovecotes Primary School's education broadband connectivity is provided through Corporate ICT through Wolverhampton Council with installation from Virgin Media.
- Dovecotes Primary School uses Lightspeed Filtering System.
    - Lightspeed blocks access to sites which could promote or include harmful and/or inappropriate behaviour or material. This includes content which promotes discrimination or extremism, drugs/substance misuse, malware/hacking, gambling, piracy and copyright theft, pro-self-harm, eating disorder and/or suicide content, pornographic content and violent material.
    - Lightspeed is a member of Internet Watch Foundation (IWF) and blocks access to illegal Child Abuse Images and Content (CAIC).
    - Lightspeed integrates 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'.
- We work with Corporate ICT to ensure that our filtering policy is continually reviewed to reflect our needs and requirements.
- If learners or staff discover unsuitable sites or material, they are required to report it immediately to the class teacher then Online Safety Lead and DSL, who will then ensure the URL is reported to the technical service.
- Filtering breaches will be reported to the Online Safety Lead, DSL (or DDSLs) and technical staff and will be recorded and escalated as appropriate.
- Parents/carers will be informed of filtering breaches involving learners as appropriate.
- Any access to material believed to be illegal will be reported immediately to the appropriate agencies, such as the IWF, the police and/or CEOP.

7.3.3 Appropriate monitoring

- We will appropriately monitor internet use on all setting-owned/internet enabled devices by:
    - Physical monitoring and supervision, including history checks;
    - SENSO active technology monitoring services - OSL, DSL and DDSLs have access.
- 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.
- If a concern is identified via monitoring approaches, we will respond in line with our safeguarding and child protection policy.

7.4 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.

When personal data is stored on any mobile device or removable media the:

- data will be encrypted, and password protected and devices will be password protected as well as protected by up-to-date endpoint (anti-virus) software
- data will be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

<u>Staff must ensure that they:</u>

- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- can help data subjects understand their rights and know how to handle a request whether verbal or written and know who to pass it to in the school
- only use encrypted data storage for personal data
- will not transfer any school personal data to personal devices. Procedures should be in place to enable staff to work from home (i.e. encrypted cloud systems)
- use personal data only on secure password-protected computers and other devices, ensuring they are properly “logged-off” when sessions end
- transfer data using encryption, a secure email account (where appropriate), and secure password protected devices.

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 and must be encrypted;

- Not downloading unapproved software or opening unfamiliar email attachments;
- Preventing, as far as possible, access to websites or tools which could compromise our systems, including anonymous browsing and other filtering bypass tools for example not disabling proxy settings whilst in school;
- The appropriate use of user logins and passwords to access our network;
    - Specific user logins and passwords will be enforced for all users (see 7.5.1).
- All users are expected to log off or lock screens/devices if systems are unattended.

7.5.1 Password policy

- All members of staff have their own unique username and private passwords to access our systems; members of staff are responsible for keeping their password private.
- From year 2 up, all learners are provided their own unique login to access systems; the first Online Safety lesson for all applicable year groups is to model how to change this such that learners are shown and encouraged how to personalise passwords and are responsible for keeping their own personal login private.
- We require all users to:
    - use strong passwords for access into our system;
    - change their passwords regularly or if they suspect it has been compromised;
    - not share passwords/login information with others or leave these for others to see;
    - not to login as another user at any time;
    - lock access to devices/systems when not in use.

7.6 Managing the safety of our website

- We will ensure that information posted on our website meets the requirements as identified by the DfE https://www.gov.uk/guidance/what-maintained-schools-must-publish-online.
- 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 for both pupils and parents as well as policies, on our website for members of the community.

7.7 Use of images and videos, including online

- We will ensure that all images and videos shared online are used in accordance with the associated policies, including (but not limited to) data security, acceptable use policies, codes of conduct/behaviour, (use on social media and use of mobile devices is covered later).
- Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website / social media / local press.

- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students / pupils in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school / academy equipment; **the personal equipment of staff should not be used for such purposes.**
- Students / pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' / pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- When children are on visits and residentials, photos of children will be added to social media on their return to school rather than during the trip/ residential visit.

Additional measures to be put in place before uploading images of pupils to social media.

1. All staff are reminded annually face-to-face, or on their induction if this is partway through the year, of their obligation to adhere to school policy and ensure that all children have parental permission before taking a picture for social media purposes and forwarding to the Senior Leadership Team for uploading to the school's social media accounts (this includes children in the background of a photo since there is still the ability to zoom in on a digital image.)
2. All staff are reminded annually, or on their induction if this is partway through the year, which children in school do not have parental photo permission (no photos permission list) and where this information is stored in school electronically to check each time a photo is sent to the Senior Leadership Team for uploading.
3. The school will limit how many children are in a photo for uploading to social media. The full names of all children will be attached when each image is sent to the Senior Leadership Team so that these can be cross referenced against the 'no photo permission' list. The photo will then be checked by two members of the Senior Leadership Team before uploading. (In the instance of a class photo, for example in case of a class assembly, this will be checked by three members of the leadership team).

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 of technology policies and the code of conduct/behaviour policy.
- Forwarding of any chain messages/emails is not permitted.
- Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email. Staff should only use recognised school email systems in relation to work.

- Setting email addresses and other official contact details will not be used to set up personal social media accounts.
- Members of the community will immediately tell the DSL if they receive offensive communication, and this will be recorded in our safeguarding files/records and dealt with by the OSL and DSL.
- Excessive social email use can interfere with teaching and learning and will be restricted; access to external personal email accounts may be blocked on site.

7.8.1 Staff email

- All members of staff are provided with an email address to use for all official communication; the use of personal email addresses by staff for any official business is not permitted.
- Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff, learners and parents.

7.8.2 Learner email

- Learners will be provided with an email account for educational purposes but used at staff discretion.
- Learners will agree an acceptable use policy and will receive education regarding safe and appropriate email etiquette before access is permitted.
- Whole-class or group email addresses may be used for communication outside of the setting, particularly in Early Years or in the event of remote/home learning.

7.9 Remote/ online learning

- This section links to the school's remote learning plan and AUPs specific to remote learning.
- Dovecotes Primary School uses a range of online learning resources, all of which have been risk assessed before being made available to learners.
- Microsoft Teams is used as the school's online learning environment. All users discuss and agree the school's AUP before use as well as the platform specific AUP to ensure expectations are known and safety is maintained.
- Parents/carers will be informed about the use of the learning environment and encouraged to support their child in contributing positively and reporting issues should they occur.
- Staff should also be aware of their role in maintaining a professional online environment.
- Should any member of staff wish to conduct a 'live' video lesson at any time (e.g. where remote learning activities are required for all or some pupils due to Covid-19), this should be discussed with senior leaders/DSL/OSL to ensure the correct systems are put in place.
- Systems are in place to ensure the correct pupils have access and other pupils cannot join teams/classes without being added by members of staff.
- Leaders and staff will regularly monitor the use of Teams to ensure appropriate and safe use. Any incidents will be reported immediately and dealt with in line with school behaviour/safeguarding & child protection policies. Any abusive/ inappropriate content will be removed immediately, and the following sanctions may apply:
    - Access 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 safeguarding and child protection procedures.

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

We use SIMs to track learners progress and share appropriate information with parents and carers.

- The Headteacher/DSL will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that use takes place 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 applies to all members of Dovecotes Primary School community.
- The term social media may include (but is not limited to) blogs, wikis, social networking sites, forums, bulletin boards, online gaming, apps, video/photo sharing sites, chatrooms and instant messenger.
- All members of Dovecotes Primary School community are expected to engage in social media in a positive and responsible manner.
  - All members of Dovecotes Primary School community are advised not to post or share content that may be considered threatening, hurtful or defamatory to others on any social media service.
- We will control learner and staff access to social media whilst using school provided devices and systems on site.

    - The use of social media on any device during teaching/contact hours for personal use is strictly prohibited.
    - The use of social media during school hours for personal use is prohibited for learners.
    - Inappropriate or excessive use of social media during school hours and/or whilst using school devices may result in removal of internet access and disciplinary/legal action.
- Concerns regarding the online conduct of any member of Dovecotes Primary School community on social media, will be reported to the DSL and be managed in accordance with our anti-bullying, allegations against staff, behaviour and child protection policies.

8.2 Staff personal use of social media

- The safe and responsible use of social media sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff, including volunteers, as part of our code of conduct and behaviour policy as well as acceptable use of technology and laptop agreements.

8.2.1 Reputation

- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the school.
    - Civil, legal or disciplinary action may be taken if staff are found to bring the profession or school into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- All members of staff are advised to safeguard themselves and their privacy when using social media services. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include, but is not limited to:
    - Setting appropriate privacy levels on their personal accounts/sites;
    - Being aware of the implications of using location sharing services;
    - Opting out of public listings on social networking sites;
    - Logging out of accounts after use;
    - Using strong passwords;
    - Ensuring staff do not represent their personal views as being that of the setting.
- Members of staff are encouraged not to identify themselves as employees of Dovecotes Primary School on their personal social networking accounts; this is to prevent information being linked with the setting and to safeguard the privacy of staff members.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online. Staff are expected to ensure that their social media use is compatible with their professional role and is in accordance our policies, and the wider professional and legal framework.

- Information and content that staff members have access to as part of their employment, including photos and personal information about learners and their family members or colleagues, will not be shared or discussed on social media sites.
- Members of staff will notify the leadership team immediately if they consider that any content shared on social media sites conflicts with an employee's role or advice in this policy.

8.2.2 Communicating with learners and parents/carers

- Staff will not use personal social media accounts to contact learners or parents/carers, nor should any contact be accepted.
- All members of staff are advised not to communicate with or add any current or past learners or family members, as 'friends' on any personal social media sites, applications or profiles.
- Any pre-existing relationships or exceptions which compromise this requirement will be discussed with the DSL.
    - Decisions made and advice provided in these situations will be formally recorded in order to safeguard learners, the setting and members of staff.
- If ongoing contact with learners is required once they have left the setting, members of staff will be expected to use existing alumni networks, or use official setting provided communication tools.
- Any communication from learners and parents received on personal social media accounts will be reported to the DSL (or DDSLs) and OSL.

8.3 Learners' 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 are not permitted for use by children under the age of 13, or in some cases higher. As such, we will not create accounts for learners under the required age as outlined in the services terms and conditions.
- Any concerns regarding learners' use of social media will be dealt with in accordance with existing policies, including anti-bullying and behaviour.
- Concerns regarding learners' use of social media will be shared with parents/carers as appropriate, particularly when concerning underage use of social media services and games.
- Learners will be advised:
    - to consider the benefits and risks of sharing personal details or information 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 appropriate adult's permission, and to only do so 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 on social media, both within the setting and externally.

8.4 Official use of social media

- Dovecotes Primary School's official social media channels are currently on Twitter with a view to assess the audience through the academic year 2021-22 and consider other social media channels. We also have a YouTube Channel, whereby videos are unlisted and pulled through the Dovecotes' school website.
- The official use of social media sites by Dovecotes Primary School only takes place with clear educational or community engagement objectives and with specific intended outcomes.
    - The official use of social media as a communication tool has been formally risk assessed and approved by the headteacher.
    - Leadership staff have access to account information and login details for our social media channels, in case of emergency, such as staff absence.
- Official social media channels have been set up as distinct and dedicated accounts for official educational or engagement purposes only.
    - Staff use school provided (class) email addresses to register for and manage official social media channels.
    - Official social media sites are suitably protected
    - Public communications on behalf of the setting will, where appropriate and possible, be read and agreed by at least one other colleague.
- Official social media use will be conducted in line with existing policies, including but not limited to anti-bullying, image/video use, data protection, confidentiality and child protection.
- All communication on official social media platforms by staff on behalf of the setting will be clear, transparent and open to scrutiny.
- Parents/carers and learners will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.
    - Only social media tools which have been risk assessed and approved as suitable for educational purposes will be used.
    - Any official social media activity involving learners will be moderated.
- Parents and carers will be informed of any official social media use with learners; written parental consent will be obtained for image and/or video content, as required.
- We will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

8.4.1 Staff expectations

- Staff are discouraged from liking or commenting on posts from the official school social media using their personal accounts as this might make them visible to parents and pupils.
- If members of staff are participating in online social media activity as part of their capacity as an employee of the setting, they will:
    - Sign our acceptable use policy, including the use of social media.
    - Be aware they are an ambassador for the setting.
    - Be professional, responsible, credible, fair and honest, and consider how the information being published could be perceived or shared.

- Always act within the legal frameworks they would adhere to within the workplace, including libel, defamation, confidentiality, copyright, data protection and equalities laws.
- Ensure appropriate consent has been given before sharing images on the official social media channel.
- Not disclose information, make commitments or engage in activities on behalf of the setting, unless they are authorised to do so.
- Not engage with any private/direct messaging with current or past learners or parents/carers.
- Inform their line manager, the DSL (or deputy) and/or the Headteacher of any concerns, such as criticism, inappropriate content or contact from learners.

9. Mobile Technology: Use of Personal Devices and Mobile Phones

- Dovecotes Primary School recognises that personal communication through mobile technologies is part of everyday life for many learners, staff and parents/carers. Mobile technology needs to be used safely and appropriately within the setting.

9.1 Expectations

- All use of mobile technology including mobile phones and personal devices such as tablets, games consoles and wearable technology will take place in accordance with our policies, including our mobile phone policy as well as our anti-bullying, behaviour and child protection policies and with the law.
- Electronic devices of any kind that are brought onto site are the responsibility of the user.
    - All members of Dovecotes Primary School community are advised to take steps to protect their mobile phones or personal devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises.
    - All members of Dovecotes Primary School community are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared.
- Mobile phones and personal devices are not permitted to be used in specific areas within and off the site including changing rooms, toilets and swimming pools.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with in line with our anti-bullying and behaviour policies.
- All members of Dovecotes Primary School community are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or would otherwise contravene our behaviour or child protection policies.

9.2 Staff use of personal devices and mobile phones

- Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as, relevant policy and procedures, including mobile phone policy, confidentiality, child protection, data security and acceptable use of technology.
- Staff will be advised to:
    - keep mobile phones and personal devices in a safe and secure place, locked away where possible, during lesson time;
    - keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times;
    - ensure that Bluetooth or other forms of communication, such as 'airdrop', are hidden or disabled during lesson times;
    - not use personal devices during teaching periods, unless permission has been given by the DSL such as in emergency circumstances;
    - ensure that any content brought onto site via mobile phones and personal devices are compatible with their professional role and expectations.
- Members of staff are not permitted to use their own personal phones or devices for contacting learners or parents and carers.
    - Any pre-existing relationships which could undermine this, will be discussed with the DSL beforehand.
- Staff will not use personal devices or mobile phones:
    - to take photos or videos of learners in line with our image use policy.
    - to work directly with learners during lessons/educational activities
    - to communicate with parents and carers.
- Where remote learning activities are required because of Covid-19, staff will use school provided equipment.
- If a member of staff breaches our policy, action will be taken in line with our staff behaviour and allegations policy.
- If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device, or have committed a criminal offence using a personal device or mobile phone, the police will be contacted and the LADO (Local Authority Designated Officer) will be informed in line with our allegations policy.

9.3 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.
- Dovecotes Primary School expects learners' personal devices/mobile phones to be:
    - handed in to the school office;
    - switched off;
    - collected from the office at home time;
    - left at the owner's risk.

- Mobile phones brought to school without permission will be confiscated and returned at the end of the day. If this becomes a regular occurrence, parents will be contacted and only returned to an adult.
- If a learner needs to contact his/her parents or carers they will must seek staff permission and inform the school office.
    - Parents are advised to contact their child via the school office.
- If a learner breaches the policy, the phone/device will be confiscated and held securely.
    - Staff may confiscate a learner's mobile phone or device if they believe it is being used to contravene our child protection, behaviour or anti-bullying policy.
    - Searches of mobile phone or personal devices will be carried out in accordance with our policy in line with the DfE 'Searching, Screening and Confiscation' guidance.'
    - Learners' mobile phones or devices may be searched by a member of the leadership team with the permission from the headteacher, with the consent of the learner and/or a parent/ carer. Content may be deleted if it contravenes our policies or the device may be handed to the police if there is suspicion it may contain illegal material.
    - Mobile phones/devices that have been confiscated will be released to parents/carers at the end of the school day once they have been informed.

9.4 Visitors' use of personal devices and mobile phones

- Parents/carers and visitors, including volunteers/contractors, are requested not to use their mobile phones while in school. Phones should be on silent or switched off and out of sight.
- Appropriate signage and information is provided on arrival to inform parents/carers and visitors of expectations of use.
- Visitors, including volunteers and contractors, who are on site for regular or extended periods of time are expected to use their mobile phones and personal devices in accordance with our acceptable use of technology policy and other associated policies, including but not limited to anti-bullying, behaviour, child protection and image use.
- Members of staff are expected to challenge visitors if they have concerns and inform the DSL (or DDSLs) of any breaches of our policy.

10. Responding to Online Safety Incidents

- All members of the Dovecotes Primary School community will be made aware of the reporting procedure for online safety concerns, including breaches of filtering, child on child abuse, including cyberbullying and youth produced sexual imagery (sexting), online sexual violence and harassment, online abuse and exploitation and illegal content.
- All members of the community will 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 with us to resolve online safety issues.
- After any investigations are completed, usually by the DSL and/or OSL, leadership staff 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 DDSLs) will seek advice from the *Mash Multi-agency Safeguarding Hub* and/or police.
- Where there is a concern that illegal activity has taken place, we will contact the police using 101, or 999 if there is immediate danger or risk of harm as appropriate.
- If information relating to a specific incident or a concern needs to be shared beyond our community, for example if other local settings are involved or the wider public may be at risk, the DSL will speak with the police and/or the Education Safeguarding Service first, to ensure that potential criminal or child protection investigations are not compromised.

10.1 Concerns about learner online behaviour and/or welfare

- The DSL (and/or DDSLs) will be informed of all online safety concerns involving safeguarding or child protection risks in line with our child protection policy.
- All concerns about learners will be recorded in line with our child protection policy.
- Dovecotes Primary School recognises that whilst risks can be posed by unknown individuals or adults online, learners can also abuse their peers; all online child-on-child abuse concerns will be responded to in line with our child protection and behaviour policies.
- The DSL (or DDSLs) will ensure that online safety concerns are investigated and reported to relevant partner agencies in line with local policies and procedures.
- Appropriate sanctions and/or pastoral/welfare support will be offered to learners as appropriate. Civil or legal action will be taken if necessary.
- We will inform parents/carers of online safety incidents or concerns involving their child, as and when required.

10.2 Concerns about staff online behaviour and/or welfare

- Any complaint about staff misuse will be referred to the DDSL (Headteacher), in accordance with our allegations against staff policy.
- Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- Appropriate disciplinary, civil and/or legal action will be taken in accordance with our staff code of conduct.
- Welfare support will be offered to staff as appropriate.

10.3 Concerns about parent/carer online behaviour and/or welfare

- Concerns regarding parents/carers' behaviour and/or welfare online will be reported to the DSL and/or (or DDSLs) and Online Safety Lead. The DSL will respond to concerns in line with existing policies, including but not limited to child protection, anti-bullying, complaints, allegations against staff, home-school agreements, acceptable use of technology and behaviour policy.
- Civil or legal action will be taken if necessary.
- Welfare support will be offered to parents/carers as appropriate.

11. Procedures for Responding to Specific Online Concerns

11.1 Online sexual violence and sexual harassment between children

- Our headteacher, DSL and appropriate members of staff have accessed and understood Ofsted's 'Review of sexual abuse in schools and colleges' (2021) recommendations and part 5 of 'Keeping Children Safe in Education' 2022
    - Full details of our response to child-on-child abuse, including sexual violence and harassment can be found in our child protection policy.
- Dovecotes Primary School takes the view that **'it could happen here'** and recognises that sexual violence and sexual harassment between children has the potential to take place online. Examples may include:
    - Non-consensual sharing of sexual images and videos;
    - Sexualised online bullying;
    - Online coercion and threats;

    - ‘Upskirting’, which typically involves taking a picture under a person’s clothing without them knowing, with the intention of obtaining sexual gratification, or causing the victim humiliation, distress or alarm – it is a criminal offence;
    - Unwanted sexual comments and messages on social media;
    - Online sexual exploitation;
- 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 any concerns relating to online sexual violence and sexual harassment, we will:
    - immediately notify the DSL (or DDSLs) and Online Safety Lead and act in accordance with our child protection and anti-bullying policies;
    - if content is contained on learners’ personal 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 implementing safety plans, offering advice on blocking, reporting and removing online content, and 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 referrals to partner agencies and/or the police;
    - if the concern involves children and young people at a different educational setting, the DSL will 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 DDSLs) will discuss this with the 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.
- Dovecotes Primary School recognises that the 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.
- Dovecotes Primary School recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
- To help minimise concerns, Dovecotes Primary School will ensure that members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment by implementing a range of age- and ability-appropriate educational methods as part of our curriculum.
- We will ensure that members of the community are aware of sources of support regarding online sexual violence and sexual harassment between learners.

11.2 Youth produced sexual imagery (“sexting”)

- Dovecotes Primary School recognises youth-produced sexual imagery ("sexting") as a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or DDSLs).
- We will follow the advice as set out in the non-statutory UKCIS guidance: Sharing nudes and semi-nudes Advice for education settings working with children and young people Responding to incidents and safeguarding children and young people.
    - Youth produced sexual imagery or 'sexting' is defined as the production and/or sharing of sexual photos and videos of and by young people who are under the age of 18. It includes nude or nearly nude images and/or sexual acts.
    - It is an offence to possess, distribute, show and make indecent images of children. The Sexual Offences Act 2003 defines a child, for the purposes of indecent images, as anyone under the age of 18.
- Dovecotes Primary School will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of creating or sharing youth produced sexual imagery 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, including the website, regarding the taking and sharing of 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 suspected youth-produced sexual imagery, unless there is no other option, or there is a clear safeguarding need or reason to do so;
        - If it is deemed necessary, the imagery will only be viewed where possible by the DSL, and any decision making will be clearly documented.
    - send, share, save or make copies of content suspected to be an indecent image/video of a child (i.e. youth-produced sexual imagery) and will not allow/request learners to.
- 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 local procedures;
    - ensure the DSL (or DDSLs) responds in line with the UKCIS guidance;
    - Store any devices containing potential youth-produced sexual imagery securely;
        - If content is contained on learners' personal devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice;
        - If a potentially 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 in line with the UKCIS guidance which considers the age and vulnerability of learners involved, including the possibility of carrying out relevant checks with other agencies;
    - inform parents/carers about the incident and how it is being managed and provide support and signposting, as appropriate;
    - make a referral to *Mash Multi-agency Safeguarding Hub* and/or the police, as deemed appropriate in line with the UKCIS guidance;

- 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;
- consider the deletion of images in accordance with the UKCIS guidance;
  - Images will only be deleted once the DSL confirms other agencies' involvement is not needed and this will not place a child at risk/compromise an investigation.
- review the handling of any incidents to ensure that best practice was implemented; the SLT will also review and update any management procedures, where necessary.

11.3 Online abuse and exploitation (including child sexual abuse and sexual or criminal exploitation)

- Dovecotes Primary School recognises online abuse and exploitation, including sexual abuse and sexual or criminal exploitation, as a safeguarding issue and all concerns will be reported to and dealt with by the DSL (or DDSLs), in line with our child protection policy.
- Dovecotes Primary School will ensure that members of the community are aware of online child abuse/sexual or criminal exploitation, including possible grooming approaches which may be employed by offenders to target learners, and understand how to respond to these.
- We will implement preventative approaches for online child abuse and exploitation via a range of age- and ability- appropriate education for learners, staff and parents/carers.
- We will ensure that members of the Dovecotes Primary School community are aware of the support available regarding online child abuse and 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 learners and other members of our community through our website.
- If made aware of an incident involving online child abuse and/or exploitation, we will:
  - act in accordance with our child protection policies and the relevant Mash procedures;
  - store any devices containing evidence securely;
    - If content is contained on learners' personal devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice;
    - If any evidence is stored on our network or devices, we will act to block access to other users and isolate the content.
  - if appropriate, make a referral to *Mash Multi-agency Safeguarding Hub* and inform the police via 101, or 999 if a learner is at immediate risk;
  - carry out a risk assessment which considers any vulnerabilities of learner(s) involved, including carrying out relevant checks with other agencies;
  - inform parents/carers about the incident and how it is being managed and provide support and signposting, as appropriate;
  - provide the necessary safeguards and support for learners, including pastoral support;
  - review the handling of any incidents to ensure that best practice is implemented; SLT will review and update any management procedures, where necessary.
- We will respond to concerns regarding online abuse and exploitation, regardless of whether the incident took place on our premises or using setting provided or personal equipment.

    - Where possible and appropriate, learners will be involved in decision making. If appropriate, they will be empowered to report concerns themselves with support, for example if the concern relates to online sexual abuse via CEOP: www.ceop.police.uk/
- If we are unclear whether a criminal offence has been committed, the DSL (or DDSLs) will obtain advice immediately through the *Mash Multi-agency Safeguarding Hub* and/or 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 police by the DSL (or DDSLs).
- If members of the public or learners at other settings are believed to have been targeted, the DSL (or DDSLs) will seek advice from *Mash Multi-agency Safeguarding Hub* and/or police before sharing information to ensure that potential investigations are not compromised.

11.4 Indecent Images of Children (IIOC)

- Dovecotes Primary School will ensure that members of the community are made aware of possible consequences of accessing Indecent Images of Children (IIOC) as appropriate.
- 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 (IWF) 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 DDSLs) will obtain advice immediately through the police and/or the *Mash Multi-agency Safeguarding Hub*.
- If made aware of IIOC, we will:
    - act in accordance with our child protection policy and the relevant Mash procedures;
    - store any devices involved securely;
    - immediately inform appropriate organisations, such as the IWF and police.
- 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 DDSL) is informed;
    - ensure that the URLs (webpage addresses) which contain the suspect images are reported to the IWF 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 IIOC have been found on setting-provided devices, we will:
    - ensure that the DSL (or DDSL) is informed;
    - ensure that the URLs (webpage addresses) which contain the suspect images are reported to the IWF via www.iwf.org.uk;
    - inform the police via 101 or 999 if there is an immediate risk of harm, and *Mash Multi-agency Safeguarding Hub*, as appropriate;
    - only store copies of images (securely, where no one else has access to them and delete all other copies) following a written request from the police;
    - report concerns, as appropriate to parents/carers.
- If made aware that a member of staff is in possession of indecent images of children on school provided devices, we will:

- ensure that the DSL (Headteacher) is informed in line with our managing allegations against staff policy;
- inform the Local 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 Online bullying

- Online bullying, along with all other forms, will not be tolerated at Dovecotes Primary School.
- Full details of how we will respond to online bullying are set out in our anti-bullying policy.

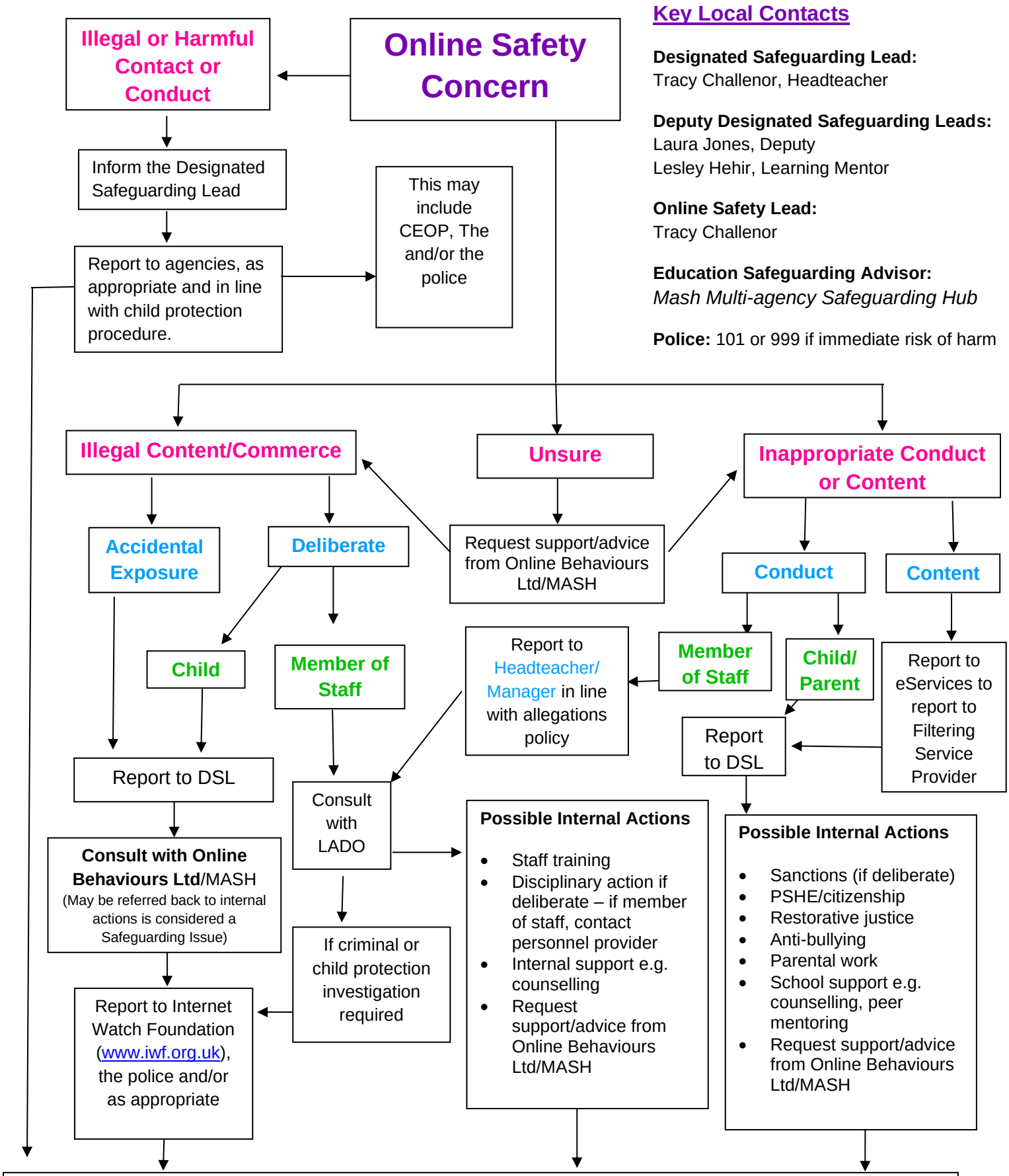
11.6 Online hate

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at Dovecotes Primary School and will be responded to in line with existing policies, including child protection, 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 DDSLs) will obtain advice through the *Mash Multi-agency Safeguarding Hub* and/or the police.

11.7 Online radicalisation and extremism

- As listed in this policy, 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.
- If we are concerned that a learner/adult may be at risk of radicalisation online, the DSL (or DDSLs) will be informed immediately, and action will be taken in line with our child protection policy.
- If we are concerned that members of staff may be at risk of radicalisation online, the DSL (Headteacher) will be informed immediately, and action will be taken in line with the child protection and allegations policies.

Responding to an Online Safety Concern Flowchart



Useful Links

National Links and Resources for Settings, Learners and Parents/carers

- CEOP:
  - www.thinkuknow.co.uk
  - www.ceop.police.uk

- Internet Watch Foundation (IWF): www.iwf.org.uk

- UK Council for Internet Safety (UKCIS): www.gov.uk/government/organisations/uk-council-for-internet-safety

- UK Safer Internet Centre: www.saferinternet.org.uk
  - Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
  - Report Harmful Content: https://reportharmfulcontent.com/

- 360 Safe Self-Review tool for schools: www.360safe.org.uk

- Childnet: www.childnet.com
  - Step Up Speak Up – Online Sexual Harassment Guidance: www.childnet.com/resources/step-up-speak-up/guidance-and-training-for-schools-and-professionals
  - Cyberbullying Guidance: www.childnet.com/resources/cyberbullying-guidance-for-schools

- Internet Matters: www.internetmatters.org

- Parent Zone: https://parentzone.org.uk

- Parent Info: https://parentinfo.org

- NSPCC: www.nspcc.org.uk/onlinesafety
  - ChildLine: www.childline.org.uk
  - Net Aware: www.net-aware.org.uk

- Lucy Faithfull Foundation: www.lucyfaithfull.org

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

- Action Fraud: www.actionfraud.police.uk

- Get Safe Online: www.getsafeonline.org