The Lanes Primary School

Online Safety Policy

(based on South West Grid for Learning (SWGfL as recommended by Notts LA)

Last reviewed	September 2022

This policy applies to all members of the school community (including staff, learners, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

Scope of the Online Safety Policy

This Online Safety Policy outlines the commitment of The Lanes Primary School to safeguard members of our school community online in accordance with statutory guidance and best practice. Schools should be aware of the legislative framework under which this Online Safety Policy template and guidance has been produced as outlined in the attached 'Legislation' Appendix.

This Online Safety Policy applies to all members of the school community (including staff, learners, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

The Lanes Primary School will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

Policy development, monitoring and review

This Online Safety Policy has been adapted from the South West Grid for Learning as recommended by Notts LA. It has been shared with staff, governors and parents/carers.

Schedule for development, monitoring and review

This Online Safety Policy was approved by the school governing body on:	October 2022
The implementation of this Online Safety Policy will be monitored by:	HT and SLT members
Monitoring will take place at regular intervals:	Termly
The governing body will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	Termly at Full Governing Body meetings
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new technological developments, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	October 2023
Should serious online safety incidents take place, the following external persons/agencies should be informed:	Notts LADO and safeguarding term/Police

Process for monitoring the impact of the Online Safety Policy

The school will monitor the impact of the policy using:

- logs of reported incidents
- monitoring logs of internet activity (including sites visited)
- internal monitoring data for network activity
- surveys/questionnaires of:
    - learners
    - parents and carers
    - staff.

Policy and leadership

Responsibilities

To ensure the online safeguarding of members of our school community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these

become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals[1] and groups within the school.

Headteacher and senior leaders

- The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety.
- The headteacher and the senior leadership team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The headteacher/senior leaders are responsible for ensuring that the office and technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
- The headteacher/senior leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.
- The headteacher/senior leaders will receive regular monitoring reports from any technical/office staff.

Governors

The DfE guidance "Keeping Children Safe in Education" states:

> "Governing bodies and proprietors should ensure there are appropriate policies and procedures in place in order for appropriate action to be taken in a timely manner to safeguard and promote children's welfare …. this includes … online safety"

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy e.g. by asking the questions posed in the UKCIS document "Online Safety in Schools and Colleges – questions from the Governing Body".

This review will be carried out by the PSS committee whose members will receive regular information about online safety incidents and monitoring reports. A member of the governing body will take on the role of Online Safety Governor to include:

- **regular meetings with the HT**
- **regularly receiving (collated and anonymised) reports of online safety incidents**
- **checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training is taking place as intended)**
- **reporting to relevant *governors group/meeting***

The governing body will also support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.

Online Safety Leads

The Online Safety Leads will be the DSL and deputies in school – Mrs J Revill, Mrs M Brown, Miss A Hodkin and Mrs L Wignell. They will liaise closely with the office staff and technical support.

The Online Safety Leads will:

- take day-to-day responsibility for online safety issues, being aware of the potential for serious child protection concerns
- have a leading role in establishing and reviewing the school online safety policies/documents
- promote an awareness of and commitment to online safety education / awareness raising across the school and beyond
- liaise with curriculum leaders to ensure that the online safety curriculum is planned, embedded and evaluated
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents
- receive reports of online safety incidents through CPOMs and create a log of incidents to inform future online safety developments
- provide (or identify sources of) training and advice for staff/governors/parents/carers/learners
- liaise with (school/local authority/MAT/external provider) technical staff and support staff (as relevant)
- meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and if possible, filtering and monitoring logs
- report at relevant governing body meetings/groups
- liaises with the local authority as appropriate

Designated Safeguarding Lead (DSL)

The DfE guidance "Keeping Children Safe in Education" states:

> "The designated safeguarding lead should take lead responsibility for safeguarding and child protection (**including online safety**). This should be explicit in the role holder's job description." … Training should provide designated safeguarding leads with a good understanding of their own role, … so they … are able to understand the unique risks associated with **online safety** and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online at school or college."

The Designated Safeguarding Lead should be trained in online safety issues and be aware of the potential for serious safeguarding issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate online contact with adults/strangers
- potential or actual incidents of grooming
- online bullying.

Curriculum Leads

Curriculum Leads will work with the Online Safety Lead to develop a planned and coordinated online safety education programme through the RSHE curriculum

This will be provided through:

- DART training in Year 6
- RHSE policies and curriculum
- assemblies and pastoral programmes
- through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

Teaching and support staff

School staff are responsible for ensuring that:

- they have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices
- they understand that online safety is a core part of safeguarding
- they have read, understood, and signed the staff acceptable use agreement (AUA)
- they immediately report any suspected misuse or problem to the DSLs for investigation/action, in line with the school safeguarding procedures
- all digital communications with learners and parents/carers should be on a professional level *and only carried out using official school systems*
- online safety issues are embedded in all aspects of the curriculum and other activities
- ensure learners understand and follow the Online Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices
- in lessons where internet use is pre-planned learners should be guided to sites checked as suitable for their use *and that processes are in place for dealing with any unsuitable material that is found in internet searches*
- where lessons take place using live-streaming or video-conferencing, staff must have full regard to national safeguarding guidance and local safeguarding policies.
- have a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.

Network manager/technical staff

The network manager/technical staff/LA is responsible for ensuring that:

- they are aware of and follow the school Online Safety Policy to carry out their work effectively in line with school policy
- the school technical infrastructure is secure and is not open to misuse or malicious attack
- the school meets (as a minimum) the required online safety technical requirements as identified by the local authority.
- there is clear, safe, and managed control of user access to networks and devices
- they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- the use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to the DSLs for investigation and action
- the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person
- monitoring software/systems are implemented and regularly updated as agreed in school policies

Learners

- are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement and Online Safety Policy
- should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

- should know what to do if they or someone they know feels vulnerable when using online technology
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

Parents and carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the online services and devices in an appropriate way.

The school will take every opportunity to help parents and carers understand these issues through:

- publishing the school Online Safety Policy on the school website
- providing them with a copy of the learners' acceptable use agreement
- publish information about appropriate use of social media relating to posts concerning the school
- seeking their permissions concerning digital images, cloud services etc
- parents'/carers' evenings, newsletters, website, social media and information about national/local online safety campaigns and literature.

Parents and carers will be encouraged to support the school in:

- reinforcing the online safety messages provided to learners in school
- the use of their children's personal devices in the school (where this is allowed – Year 6 only)

- the production/review/monitoring of the school Online Safety Policy/documents
- the production/review/monitoring of the school filtering policy (if possible and if the school chooses to have one) and requests for filtering changes
- mapping and reviewing the online safety education provision – ensuring relevance, breadth and progression and coverage
- reviewing network/filtering/monitoring/incident logs, where possible
- encouraging the contribution of learners to staff awareness, emerging trends and the school online safety provision
- consulting stakeholders – including staff/parents/carers about the online safety provision

Professional Standards

There is an expectation that required professional standards will be applied to online safety as in other aspects of school life i.e., policies and protocols are in place for the use of online communication technology between the staff and other members of the school and wider community, using officially sanctioned school mechanisms.

Policy

Online Safety Policy

The DfE guidance "Keeping Children Safe in Education" states:

> **"Online safety** and the school or college's approach to it should be reflected in the child protection policy"

The school Online Safety Policy:

- sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication
- allocates responsibilities for the delivery of the policy
- is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours
- establishes guidance for staff in how they should use digital technologies responsibly, protecting themselves and the school and how they should use this understanding to help safeguard learners in the digital world
- describes how the school will help prepare learners to be safe and responsible users of online technologies
- establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms
- is supplemented by a series of related acceptable use agreements
- is made available to staff at induction and through staff meetings, training, briefings, email
- is published on the school website.

Acceptable use

Acceptable use policies and procedures are shared annually with all staff. New starters at school receive copies of all documents and relevant training.

The Online Safety Policy and acceptable use agreements define acceptable use at the school. The acceptable use agreements will be communicated/re-enforced through:

- staff induction and handbook
- Policies – Acceptable Use, Data Handling and security, CPOMs Protocol, Code of Conduct, Security Incidents Policy, training Powerpoints and documents. These are shared annually with all staff and governors. Policies are on the school website.
- posters/notices around where technology is used
- communication with parents/carers
- built into education sessions
- school website
- peer support.

When using communication technologies, the school considers the following as good practice:

- when communicating in a professional capacity, staff should ensure that the technologies they use are officially sanctioned by the school
- any digital communication between staff and learners or parents/carers (e-mail, social media, learning platform, etc.) must be professional in tone and content. Personal e-mail addresses, text messaging or social media must not be used for these communications.
- staff should be expected to follow good practice when using personal social media regarding their own professional reputation and that of the school and its community
- users should immediately report to a nominated person – in accordance with the school policy – the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication
- relevant policies and permissions should be followed when posting information online e.g., school website and social media. Only school e-mail addresses should be used to identify members of staff and learners.

Reporting and responding

The 2021 Ofsted "Review of Sexual Abuse in Schools and Colleges" highlighted the need for schools to understand that reporting systems do not always respond to the needs of learners. While the report looks specifically at harmful sexual behaviours, schools may wish to address these issues more generally in reviewing their reporting systems. The Ofsted review suggested:

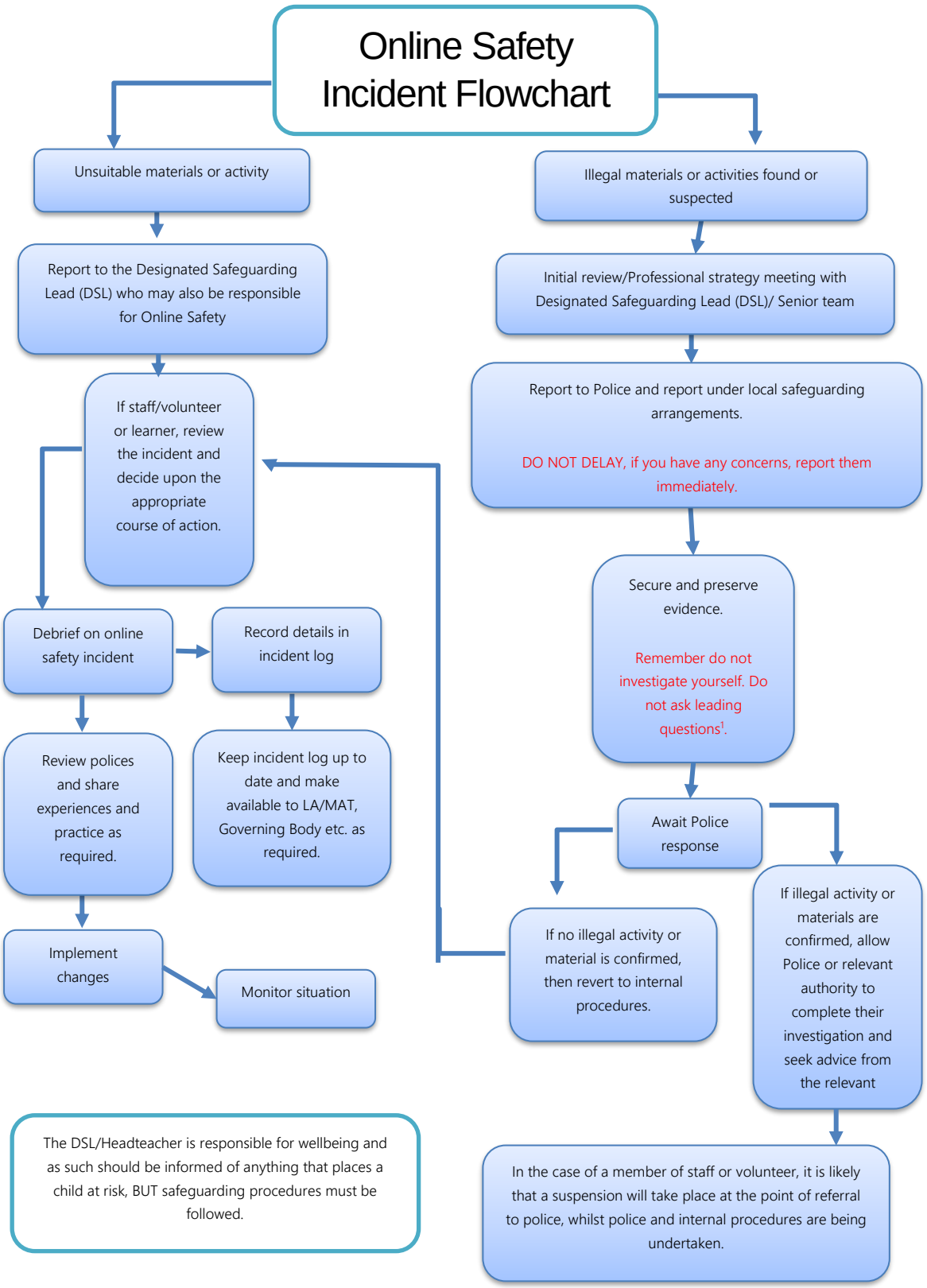
> *"School and college leaders should create a culture where sexual harassment and online sexual abuse are not tolerated, and where they identify issues and intervene early to better protect children and young people. ..In order to do this, they should assume that sexual harassment and online sexual abuse are happening in their setting, even when there are no specific reports, and put in place a whole-school approach to address them. This should include:*
>
> - *routine record-keeping and analysis of sexual harassment and sexual violence, including online, to identify patterns and intervene early to prevent abuse"*

The school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

- there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.
- all members of the school community will be made aware of the need to report online safety issues/incidents
- reports will be dealt with as soon as is practically possible once they are received
- the Designated Safeguarding Leads and other responsible staff have appropriate skills and training to deal with online safety risks.
- if there is any suspicion that the incident involves any illegal activity or the potential for serious harm the incident must be escalated through the agreed school safeguarding procedures.
- any concern about staff misuse will be reported to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of Governors and the local authority.
- where there is no suspected illegal activity, devices may be checked using the following procedures:
    - one or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
    - conduct the procedure using a designated device that will not be used by learners and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.
    - ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
    - record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed, and attached to the form
    - once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
        - internal response or discipline procedures
        - involvement by local authority
        - police involvement and/or action

- it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
- there are support strategies in place e.g., peer support for those reporting or affected by an online safety incident
- incidents should be logged confidentially.
- relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; Professionals Online Safety Helpline; Reporting Harmful Content; CEOP.
- those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions
- learning from the incident (or pattern of incidents) will be provided (as relevant and anonymously) to:
    - *staff, through regular briefings*
    - *learners, through assemblies/lessons*
    - *parents/carers, through newsletters, school social media, website*
    - *governors, through regular safeguarding updates*
    - *local authority/external agencies, as relevant*
    - The school will make the flowchart below available to staff to support the decision-making process for dealing with online safety incidents.

Online Safety Incident Flowchart



The DSL/Headteacher is responsible for wellbeing and as such should be informed of anything that places a child at risk, BUT safeguarding procedures must be followed.

School actions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as set out by Notts LA and the school behaviour policy.

Online Safety Education Programme

While regulation and technical solutions are particularly important, their use must be balanced by educating learners to take a responsible approach. The education of learners in online safety is therefore an essential part of the school's online safety provision. Learners need the help and support of the school to recognise and avoid online safety risks and develop their resilience.

The 2021 Ofsted "Review of Sexual Abuse in Schools and Colleges" highlighted the need for:

> *"a carefully sequenced RSHE curriculum, based on the Department for Education's (DfE's) statutory guidance, that specifically includes sexual harassment and sexual violence, including online. This should include time for open discussion of topics that children and young people tell us they find particularly difficult, such as consent and the sending of 'nudes'.."*

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

A planned online safety curriculum for all year groups is regularly taught in a variety of contexts.

- Lessons are matched to need; are age-related and build on prior learning
- Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes
- Learner need and progress are addressed through effective planning and assessment
- Digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas e.g. RHSE; SRE; etc
- it incorporates/makes use of relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week
- the programme will be accessible to learners at different ages and abilities such as those with additional learning needs or those with English as an additional language.
- *learners should be helped to understand the need for the learner acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school*
- *staff should act as good role models in their use of digital technologies the internet and mobile devices*
- *in lessons where internet use is pre-planned, it is best practice that learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches*
- *where learners are allowed to freely search the internet, staff should be vigilant in supervising the learners and monitoring the content of the websites the young people visit*
- *it is accepted that from time to time, for good educational reasons, students may need to research topics, (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff should be able to request the temporary removal of those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need*

- **the online safety education programme should be relevant and up to date to ensure the quality of learning and outcomes.**

Contribution of Learners

The school acknowledges, learns from, and uses the skills and knowledge of learners in the use of digital technologies. We recognise the potential for this to shape the online safety strategy for the school community and how this contributes positively to the personal development of young people. Their contribution is recognised through:

- mechanisms to canvass learner feedback and opinion.
- appointment of digital leaders/ambassadors/school councillors
- learners contribute to the online safety education programme e.g. peer education, digital leaders leading lessons for younger learners, online safety campaigns
- learners designing/updating acceptable use agreements
- contributing to online safety events with the wider school community e.g. parents' evenings, family learning programmes etc.

Staff/volunteers

The DfE guidance "Keeping Children Safe in Education" states:

> "All staff should receive appropriate safeguarding and child protection training (**including online safety**) at induction. The training should be **regularly updated**. In addition, all staff should receive safeguarding and child protection (**including online safety**) updates (for example, via email, e-bulletins, and staff meetings), as required, and at least annually, to continue to provide them with relevant skills and knowledge to safeguard children effectively."
>
> "Governing bodies and proprietors should ensure... that safeguarding training for staff, **including online safety** training, is integrated, aligned and considered as part of the whole school or college safeguarding approach and wider staff training and curriculum planning.**"**

All staff will receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- a planned programme of formal online safety and data protection training will be made available to all staff. This will be regularly updated and reinforced.
- the training will be an integral part of the school's annual safeguarding and data protection training for all staff
- all new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements. It includes explicit reference to classroom management, professional conduct, online reputation and the need to model positive online behaviours
- the Designated Safeguarding Lead (or other nominated person) will receive regular updates through attendance at external training events, (e.g. LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations
- this Online Safety Policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days
- the DSLs will provide advice/guidance/training to individuals as required.

Governors

Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any sub-committee/group involved in technology/online safety/health and safety/safeguarding. This may be offered in several ways such as:

- attendance at training provided by the local authority or other relevant organisation
- participation in school training / information sessions for staff or parents (this may include attendance at assemblies/lessons).

A higher level of training will be made available to (at least) the Online Safety Governor.

Families

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will seek to provide information and awareness to parents and carers through:

- regular communication, awareness-raising and engagement on online safety issues, curriculum activities and reporting routes
- regular opportunities for engagement with parents/carers on online safety issues through awareness workshops / parent/carer evenings etc
- the learners – who are encouraged to pass on to parents the online safety messages they have learned in lessons and by learners leading sessions at parent/carer evenings.
- letters, newsletters, website, learning platform,
- high profile events / campaigns e.g. Safer Internet Day
- reference to the relevant web sites/publications,
- Sharing good practice with other schools in clusters and or the local authority

Adults and Agencies

The school will provide opportunities for local community groups and members of the wider community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- online safety messages targeted towards families and relatives.
- the school will provide online safety information via their website for the wider community

Technology

The school is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. The school should ensure that all staff are made aware of policies and procedures in place on a regular basis and explain that everyone is responsible for online safety and data protection.

Filtering – managed by Hancox IT

- the school filtering policies are agreed by senior leaders and technical staff (Hancox IT) and are regularly reviewed and updated in response to changes in technology and patterns of online safety incidents/behaviours
- the school manages access to content across its systems for all users. The filtering provided meets the standards defined in the UK Safer Internet Centre Appropriate filtering.
- access to online content and services is managed for all users
- illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated
- there are established and effective routes for users to report inappropriate content
- there is a clear process in place to deal with requests for filtering changes
- the school has (if possible) provided enhanced/differentiated user-level filtering (allowing different filtering levels for different abilities/ages/stages and different groups of users: staff/learners, etc.)
- younger learners will use child friendly/age-appropriate search engines
- where personal mobile devices have internet access through the school network, content is managed in ways that are consistent with school policy and practice.
- access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with school policy and practice.

The DfE guidance "Keeping Children Safe in Education" states:

> "It is essential that governing bodies and proprietors ensure that appropriate filters and monitoring systems are in place ...governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the … risks from the school's or college's IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filters and monitoring systems in place and regularly review their effectiveness. They should ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified. "

The school has monitoring systems in place to protect the school, systems and users:

- The school monitors all network use across all its devices and services.
- An appropriate monitoring strategy for all users has been agreed and users are aware that the network is monitored. There is a staff lead responsible for managing the monitoring strategy and processes.
- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention. Management of serious safeguarding alerts is consistent with safeguarding policy and practice
- Technical monitoring systems are up to date and managed and logs/alerts are regularly reviewed and acted upon.

The school follows the UK Safer Internet Centre Appropriate Monitoring guidance and protects users and school systems through the use of the appropriate blend of strategies strategy informed by the school's risk assessment. These may include:

- physical monitoring (adult supervision in the classroom)
- internet use is logged, regularly monitored and reviewed
- filtering logs are regularly analysed and breaches are reported to senior leaders
- *pro-active alerts inform the school of breaches to the filtering policy, allowing effective intervention.*
- *where possible, school technical staff regularly monitor and record the activity of users on the school technical systems*
- *use of a third-party assisted monitoring service to review monitoring logs and report issues to school monitoring lead(s)*

Technical Security

The school technical systems will be managed in ways that ensure that the school meets recommended technical requirements there will be regular reviews and audits of the safety and security of school technical systems

- servers, wireless systems and cabling are securely located and physical access restricted
- there are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud.
- all users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager (Hancox IT) and will be reviewed, at least annually.
- all users (adults and learners) have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details. Users must immediately report any suspicion or evidence that there has been a breach of security
- all school networks and system will be protected by secure passwords. Passwords must not be shared with anyone. All users will be provided with a username and password by Hancox IT who will keep an up-to-date record of users.
- the master account passwords for the school systems are kept by Hancox IT
- Jo Gosling is responsible for ensuring that all software purchased by and used by the school is adequately licenced and that the latest software updates (patches) are applied**.**
- an appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed
- appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems and devices from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date endpoint (anti-virus) software.
- an agreed policy is in place that allows staff to/forbids staff from downloading executable files and installing programmes on school devices
- an agreed policy is in place regarding the use of removable media (e.g., memory sticks/CDs/DVDs) by users on school devices.
- systems are in place that prevent the unauthorised sharing of personal data unless safely encrypted or otherwise secured

Mobile technologies

The DfE guidance “Keeping Children Safe in Education” states:

"The school or college should have a clear policy on the use of mobile and smart technology. Amongst other things this will reflect the fact many children have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G). This access means some children, whilst at school or college, sexually harass, bully, and control others via their mobile and smart technology, share indecent images consensually and non-consensually (often via large chat groups) and view and share pornography and other harmful content. Schools and colleges should carefully consider how this is managed on their premises and reflect this in their mobile and smart technology policy and their child protection policy.

Mobile technology devices may be school owned/provided or personally owned and might include smartphone, tablet, wearable devices, notebook/laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school learning platform and other cloud-based services such as e-mail and data storage.

All users should understand that the primary purpose of the use of mobile/personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school polices including but not limited to those for safeguarding, behaviour, anti-bullying, acceptable use, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's online safety education programme.

School owned/provided devices:

Personal devices

- *which users are allowed to use personal mobile devices in school (staff/learners/visitors)*
- *restrictions on where, when and how they may be used in school*
- *if used in support of learning, how staff will plan their lessons around the potential variety of device models and different operating systems*
- *storage*
- *whether staff will be allowed to use personal devices for school business*
- *levels of access to networks/internet (e.g., access, or not, to internet/guest wi-fi/network)*
- *network/broadband capacity*
- *technical support (this may be a clear statement that no technical support is available)*
- *filtering of the internet connection to these devices and monitoring the access*
- *management of software licences for personally owned devices.*
- *data protection*
- *taking/storage/use of images*
- *liability for loss/damage or malfunction following access to the network (likely to be a disclaimer about school responsibility)*
- *identification/labelling of personal devices*
- *how visitors will be informed about school requirements*
- *how education about the safe and responsible use of mobile devices is included in the school online safety education programmes*
- *how misuse will be dealt with*

Social media

With widespread use of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of learners, the school and the individual when publishing any material online.

Expectations for teachers' professional conduct are set out in the DfE Teachers Standards but all adults working with children and young people must understand that the nature and responsibilities of their work place them in a position of trust and that their conduct should reflect this.

All schools and local authorities have a duty of care to provide a safe learning environment for learners and staff. Schools could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, bully online, discriminate on the grounds of sex, race, or disability or who defame a third party may render the school liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to learners through:

- ensuring that personal information is not published
- education/training being provided including acceptable use, age restrictions, social media risks, digital and video images policy, checking of settings, data protection and reporting issues
- clear reporting guidance, including responsibilities, procedures and sanctions
- risk assessment, including legal risk
- guidance for learners, parents/carers

School staff should ensure that:

- no reference should be made in social media to learners, parents/carers or school staff
- they do not engage in online discussion on personal matters relating to members of the school community
- personal opinions should not be attributed to the school
- security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information
- they act as positive role models in their use of social media

When official school social media accounts are established, there should be:

- a process for approval by senior leaders
- clear processes for the administration, moderation, and monitoring of these accounts – involving at least two members of staff
- a code of behaviour for users of the accounts
- systems for reporting and dealing with abuse and misuse
- understanding of how incidents may be dealt with under school disciplinary procedures.

Personal use

- personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the school it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy

- personal communications which do not refer to or impact upon the school are outside the scope of this policy
- where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- *the school permits reasonable and appropriate access to personal social media sites during school hours*

Monitoring of public social media

- As part of active social media engagement, the school may pro-actively monitor the Internet for public postings about the school
- the school should effectively respond to social media comments made by others according to a defined policy or process
- when parents/carers express concerns about the school on social media we will urge them to make direct contact with the school, in private, to resolve the matter. Where this cannot be resolved, parents/carers should be informed of the school complaints procedure.

Digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and learners instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and learners need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees.

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm

- when using digital images, staff will inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images.
- staff/volunteers must be aware of those learners whose images must not be taken/published. Those images should only be taken on school devices. The personal devices of staff should not be used for such purposes
- 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 *learners* 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, storage, distribution and publication of those images
- care should be taken when sharing digital/video images that learners are appropriately dressed
- learners must not take, use, share, publish or distribute images of others without their permission
- photographs published on the website, or elsewhere that include learners will be selected carefully and will comply with Online Safety Policy
- written permission from parents or carers will be obtained before photographs of learners are taken for use in school or published on the school website/social media.
- parents/carers will be informed of the purposes for the use of images, how they will be stored and for how long – in line with the school data protection policy

- images will be securely stored in line with the school retention policy
- learners' work can only be published with the permission of the learner and parents/carers.

Online Publishing

The school communicates with parents/carers and the wider community and promotes the school through:

- Public-facing website
- Online newsletters
- Seesaw app
- Year group emails

The school website is managed/hosted by Primary Site. The school ensures that online safety policy has been followed in the use of online publishing e.g., use of digital and video images, copyright, identification of young people, publication of school calendars and personal information – ensuring that there is least risk to members of the school community, through such publications.

Where learner work, images or videos are published, their identities are protected, and full names are not published.

The school public online publishing provides information about online safety e.g., publishing the schools Online Safety Policy and acceptable use agreements; curating latest advice and guidance; news articles etc, creating an online safety page on the school website.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

The school:

- has a Data Protection Policy based on the LA model.
- implements the data protection principles and can demonstrate that it does so
- has paid the appropriate fee to the Information Commissioner's Office (ICO)
- has appointed an appropriate Data Protection Officer (DPO) who has effective understanding of data protection law and is free from any conflict of interest.
- has a 'Record of Processing Activities' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it
- the Record of Processing Activities lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis is listed
- has an 'information asset register' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it
- information asset register lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis will have also been listed
- will hold the minimum personal data necessary to enable it to perform its function and will not hold it for longer than necessary for the purposes it was collected for. The school 'retention schedule" supports this

- data held is accurate and up to date and is held only for the purpose it was held for. Systems are in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals
- provides staff, parents, volunteers, teenagers, and older children with information about how the school looks after their data and what their rights are in a clear Privacy Notice (see Privacy Notice section in the appendix)
- has procedures in place to deal with the individual rights of the data subject, e.g. one of the dozen rights applicable is that of Subject Access which enables an individual to see/have a copy of the personal data held about them
- carries out Data Protection Impact Assessments (DPIA) where necessary e.g. to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier
- has undertaken appropriate due diligence and has data protection compliant contracts in place with any data processors
- understands how to share data lawfully and safely with other relevant data controllers.
- has clear and understood policies and routines for the deletion and disposal of data
- reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach as required by law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents
- has a Freedom of Information Policy which sets out how it will deal with FOI requests
- provides data protection training for all staff at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff

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

- data will be encrypted, and password protected.
- device will be password protected.
- device will be 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**.**

Staff must ensure that they:

- 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. Work laptops and IPads are provided.
- use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data
- transfer data using encryption, a secure email account (where appropriate), and secure password protected devices.

Outcomes

The impact of the Online Safety Policy and practice is regularly evaluated through the review/audit of online safety incident logs; behaviour/bullying reports; surveys of staff, learners; parents/carers and is reported to relevant groups:

- there is balanced professional debate about the evidence taken from the reviews/audits and the impact of preventative work e.g., online safety education, awareness, and training
- there are well-established routes to regularly report patterns of online safety incidents and outcomes to school leadership and Governors
- parents/carers are informed of patterns of online safety incidents as part of the school's online safety awareness raising
- online safety (and related) policies and procedures are regularly updated in response to the evidence gathered from these reviews/audits/professional debate
- the evidence of impact is shared with other schools, agencies and LAs to help ensure the development of a consistent and effective local online safety strategy.

Appendix

A1 - Acceptable Personal Use of Resources and Assets Policy

A2 - The lanes E- Safety Policy

A3 - The Lanes Use of Children's Images Policy

A4 – GDPR Summary Letter

A5 – GDPR Photo Consent Form

A6 - The Lanes Home School Agreement

A7 - Responding to incidents of misuse -flow chart

A8 - Record of reviewing devices/internet sites (responding to incidents of misuse)

A9 – Reporting Log

A1

Acceptable Personal Use of Resources and Assets Policy

Explaining what is acceptable use of resources and assets provided by us, including IT facilities and covering personal use

Policy points are numbered. The numbering corresponds to explanations of 'why?' and 'how?' for each point further down the page.

What must I do?

1. ***MUST:*** You must use our facilities economically; your personal use must not create extra costs for us

2. ***MUST NOT:*** You must not use our facilities to undertake any unlawful, libellous, immoral or offensive activities, including accessing, downloading, storing, creating, copying or disseminating offensive material. This includes, but is not limited to, pornographic, sexual, violent or criminal content and racist, sexist or otherwise discriminatory material

3. ***MUST NOT:*** Personal use must not interfere with your productivity and how you carry out your duties

4. ***MUST NOT:*** Personal use must not reflect adversely on our reputation

5. ***MUST NOT:*** You must not leave personal-use websites open during your working time, even if they are minimised on your screen and you are not actively viewing/ using them

6. ***MUST NOT:*** You must not use browsers or access/ attempt to access sites that are knowingly unacceptable, even if this is in your own time

7. ***MUST NOT:*** You must not send or forward chain, joke or spam emails

8. ***MUST NOT:*** You must not use the Organisation's facilities for commercial purposes not approved by us or for personal financial gain

9. ***MUST NOT:*** You must not use your access rights or identity as an employee to mislead another person, for personal gain or in any other way which is inconsistent with your role

10. ***MUST NOT:*** You must not disclose (in writing, speech or electronically) information held by us unless you are authorised to do so, and the recipients are authorised to receive it

11. ***MUST NOT:*** When you print, photocopy, scan or fax official-sensitive information, you must not leave the information unattended.

12. **MUST NOT:** You must not connect any equipment to our IT network that has not been approved

13. ***MUST NOT:*** You must not do anything that would compromise the security of the information held by us, such as downloading/ spreading any harmful virus/ program or disabling or changing standard security settings

14. ***MUST NOT:*** You must not make personal use of the information available to you that is not available to the public

Why must I do it?

1. ALL: To ensure we use our IT and other facilities resources effectively, making sure that our reputation is

maintained and to ensure that staff working time is used efficiently on delivering our business outcomes

How must I do it?

1. By checking with your manager or where you have any uncertainty over what is appropriate
2. By complying with the points of this policy
3. You must only make personal use of our IT facilities outside of time you are recording or is designated as your 'working hours'
4. By complying with the points of this policy
5. Closing websites when you are not actively using them
6. By taking care over the sites you are about to open, including reading search report information before opening
7. By deleting such items if you receive them.
8. By checking with your manager where you have any uncertainty over what is appropriate
9. By checking with your manager where you have any uncertainty over what is appropriate
10. If you are not sure if you are authorised to disclose information, speak with your manager in the first instance
11. If you are faxing information outside your immediate office, always make sure that there is someone waiting at the other end to receive it. For other devices, if there is no secure release facility which requires you to be present, you must ensure you wait for the process to complete and remove any originals and copies from the equipment.
12. Check that equipment has been tagged or marked as an accepted and managed device before insertion/ connection.
13. IT controls should prevent your ability to download anything harmful, but if in doubt, contact your manager in the first instance.
14. If you wish to utilise Organisation data in a personal capacity, you must make a formal request for information to the Organisation.

A2 The Lanes E-Safety Policy

1. Introduction

- At The Lanes Primary School we are committed to:

  - Developing outstanding teaching and learning
  - Having the highest expectations of all our pupils and knowing our children well.
  - Challenging all children to strive for academic, creative, sporting and personal accomplishment within a broad, vibrant and enriched curriculum.
  - Developing a truly inclusive school, where all children can flourish whatever their background, abilities, religion, gender or beliefs.
  - Celebrating achievement in all areas, valuing academic, creative, sporting and personal development equally.
  - Fostering an ethos of respect and empathy
  - Instilling a lifelong love of learning and a strong grounding for future success.
  - Ensuring that children feel secure and happy.

We celebrate perseverance; resilience and risk taking, ensuring children welcome challenge and are not frightened to make mistakes. We encourage children to take ownership of and responsibility for their learning, so they have the confidence and curiosity to ask questions, solve problems and respond to quality feedback. Children are praised for hard work, determination and having a positive attitude. We encourage the children to be proud of the school and their achievements in all areas of the curriculum. We foster open and honest communication with parents and actively seek to engage with all members of the community in a positive and collaborative manner

- We aim to achieve our mission by being inclusive, maintaining a safe and stimulating learning environment, securing outstanding learning and teaching, delivering our Irresistible Curriculum, following a values-based approach and working with parents, carers and the wider community.

- We believe that E-Safety both supports and strengthens what we aim to do in every aspect of school life. Our commitment to the welfare of our children and the upholding of our Safeguarding policy must be reflected through our implementation of the E-Safety policy.

2. Policy Scope

- This policy applies to all members of the School community (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of the school computing systems, both in and out of school.

- The Education and Inspections Act 2006 empowers the Head teacher to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other E- Safety incidents covered by this policy, which may take place outside of the school, but are linked to membership of the school.

3. Policy Development

This E-Safety policy has been developed by the E-Safety Coordinator and Computing Curriculum team, in consultation with the Head teacher and the Governors (see Appendix 1 for details of these).

4. Policy Aims

The aim of this policy is to ensure that we safeguard our children against potential incidents of bullying, grooming, radicalisation or abuse through their use of technology. We aim to educate our children to use technology responsibly and safely, preventing them from either becoming victims of perpetrators of online abuse, whilst also treating equipment with respect and care. Through this policy, we aim to ensure that all members of the school community recognise and fulfil their shared commitment to E Safety.

5. Equal Opportunities

- The Lanes Primary School is committed to equality of opportunity, and to promoting an ethos of dignity, courtesy and respect throughout the organisation. For further information, please refer to the Equality policy.

- Every effort will be made to ensure that a fair and consistent practice, as detailed in this policy and procedure, is carried out.

6. Monitoring

The quality of E-Safety delivery at The Lanes Primary School will be assured by:

- Ensuring this policy is disseminated and adhered to.

- Monitoring the impact of the policy as set out in section 12.

- Addressing any underperformance in a timely manner, whether it has come to light through the monitoring procedures outlined in this policy or as a result of other school monitoring mechanisms.

7. Roles and Responsibilities

The delivery of the E-Safety policy is a collective responsibility. The following section outlines the roles and responsibilities of individuals and groups within the School in relation to E-Safety.

7.1 The Governing Body

7.11 There will be a designated E-Safety Governor who will support the school and the E-Safety Coordinator in approving, monitoring and reviewing the effectiveness of the policy.

7.12 The designated E-Safety Governor will review this policy on an annual basis and support the Principal and Senior Leadership Team (see Appendix 1) in their implementation of the policy through termly review meetings.

7.1 The Head teacher and Senior Leaders

7.11 The Head teacher and (at least) another member of the Senior Leadership Team should be informed immediately in the event of an online safety allegation being made against a memberof staff and follow the procedure as discussed.

7.12 The Head teacher has a duty of care for ensuring the safety (including online safety) of members of the School community, though the day to day responsibility for online safety will be delegated to the E-Safety Coordinator.

7.13They will ensure that they keep up to date with statutory requirements and recommendations in relation to E-Safety.

7.14 The Head teacher has overall responsibility for the data and data security and willensure that the school is GDPR compliant. There is a named Data Protection officer in school.

7.15 They will support and hold to account the E-Safety Coordinator in carrying out the responsibilities outlined in 7.3.

7.16 They will report on the quality of E-Safety provision to the Governing Body in the Head teacher's report.

7.17 They will strive to provide suitable resources and training to support the aims of this policy.

7.2 The E-Safety Coordinator

7.2.1 The E-Safety Coordinator will promote an awareness and commitment to e-safeguarding throughout the School community.

7.2.2 They will take day-to-day responsibility for online safety issues and have a leading rolein establishing and reviewing the Schools E-Safety policy.

7.2.3 They will ensure that E-Safety is embedded across the curriculum.

7.2.4 The E-Safety Coordinator will ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.

7.2.5 They will receive reports of online safety incidents and use the incident reports to inform future online safety developments.

7.2.6 They will communicate termly with the E-Safety Governor to discuss current issues and to review incident logs.

7.27 They will report half-termly to the Senior Leadership Team.

7.28 They will regularly research updates in E-Safety issues and legislation and know the potential for serious child protection issues that may arise from online misuse, including radicalisation

7.3 **The Computing Curriculum Team**

7.3.1 The Computing Curriculum Team will oversee the delivery of the E-Safety element of the Computing curriculum.

7.4 **Technical Staff**

7.4.1 The technical staff will report any E-Safety related issues that arise to the E-Safety Coordinator.

7.4.2 They will ensure that the School's technical infrastructure is secure and is not open to misuse or malicious attack.

7.4.3 They will ensure that the School meets required online safety technical requirements and any E-Safety policy that may apply.

7.4.4 They will ensure that the Local Authority web filtering policy is applied and updated on a regular basis.

7.4.5 They will ensure that all documentation relating to the School's e-security is up-to-date.

7.5 **All Staff**

All staff are responsible for ensuring that they have read, understood, signed and help promote the Staff, Governor and Volunteer Acceptable Use Agreement (see Appendix 2).

7.6 **Teaching Staff**

All teaching staff are responsible for ensuring that:

7.6.1 Online safety teaching is part of all computing lessons and is embedded in all aspects of the curriculum and other activities.

7.6.2 Pupils understand and follow the E-Safety policy and all acceptable use policies.

7.6.3 They monitor the use of digital technologies, mobile devices, cameras etc. in the school and implement current policies about these devices.

7.7 **Our Children**

All of our children will be responsible for using the School's digital technology systems in accordance with the Pupil Acceptable Use Agreements in our Home School Agreement. (see Appendix 3).

7.8 **Parents and Carers**

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way.

7.8.1 They will have access to this policy and supportive materials concerning E-Safety at home and these will be made available to them via the School's website.

7.8.2 Parents/carers should consult with the School if they have concerns about their child or other children's use of technology inside and outside of the School if related to their membership of the School. The school will inform parents of any concerns with an e safety 'bump note' (see Appendix 4).

7.8.3 They will support the Pupil Acceptable Use Agreements by signing the Home School Agreement.

7.9 **Community Users and Volunteers**

Community Users and volunteers who access School systems or the website as part of the wider School provision will be expected to read, understand, sign and help promote the Staff, Governor and Volunteer Acceptable Use Agreement (see Appendix 5).

Procedures

8 Time Allocation

8.1 The School has a commitment to ensure that all children in Years 1-6 have access to a Computing lesson every week. Within every Computing lesson, it is required that E-Safety is referred to. One lesson each half term is designated to the explicit teaching of E-Safety. Children in Reception are taught to use technology safely as part of the Early Years curriculum.

8.2 Every term, there will be an E-Safety assembly for the whole School but these may be delivered separately to each Key Stage (as appropriate) to ensure our children access age- appropriate content.

8.3 The School will participate in Safer Internet Day annually, with every child taking part in activities relating to E-Safety.

9 Planning

9.1 E-Safety must be planned into every Computing lesson and reviewed regularly in line with new initiatives and laws.

10 Teaching and Learning

10.1 The school internet access will be designed expressly for pupil use and will include filtering appropriate to the age of the pupils.

10.2 Pupils will be taught what internet use is acceptable and what is notand given clear objectives for internet use.

10.3 Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

10.4 Pupils will be shown how to publish and present information to a wider audience.

10.5 Pupils will be taught the importance of cross-checking information before accepting its accuracy.

10.6 Pupils will be taught how to be kind, when commenting online, using apps or games.

11 Assessment, Recording and Reporting

11.1 Staff are responsible for being familiar with procedures to report any incidents.

11.2 All incidents should be recorded and the correct people notified.

11.3 As soon as an incident is recorded, the E-Safety Coordinator should also be made aware, face to face, as a matter of urgency.

11.4 For cases of Cyber-bullying, please refer to the Anti-Bullying Policy.

12 Monitoring and Evaluation

12.1 The Governing body will be reported to by the Head teacher once a term via the Head teacher's report.

12.2 The E-Safety Coordinator and computing team will monitor the implementation of the policy by checking for reported incidents, scrutinising Computing planning to check for coverage and carrying out staff and pupil questionnaires annually.

13 Review of the Policy

13.1 The Governing Body will review the E-Safety policy every academic year at its Pupils Standards and Strategy meeting prior to it being presented to the full Governing Body.

13.2 The Governing Body will take account of the Head teacher's report in its review of the E- Safety policy.

13.3 Following the monitoring and evaluation processes set out in section 10, the E-Safety policy will be revised as required by the E-Safety Coordinator, Computing Curriculum team, the Head teacher and Senior Leadership Team to ensure that it is effective.

13.4 The E-Safety policy will be revised by the E-Safety Coordinator and Computing Curriculum team to introduce any changes in regulation and statutory guidance to ensure that it is always up to date.

What if I need to do something against the policy?

If you believe you have a valid business reason for an exception to these policy points, having read and understood the reasons why they are in place, please raise a formal request by contacting the school office.

Document Control
Version: 2
Date approved: Autumn 2021
Approved by: FGB
Next review: Autumn 2022
References

- Data Protection Act 2018
- General Data Protection Regulations 2016

Breach Statement
Breaches of Information Policies will be investigated and may result in disciplinary action. Serious breaches of Policy may be considered gross misconduct and result in dismissal without notice, or legal action being taken against you.

A3 THE LANES PRIMARY SCHOOL POLICY FOR USE OF CHILDREN'S IMAGES IN SCHOOL AND FOR PUBLICITY PURPOSES

Introduction

The word images is used here to include photographs, digital photographs, webcam, mobile phones, film and video recordings.

The Lanes Primary School believes that the responsible use of children's images can make a valuable contribution to the life and morale of the school. The use of photographs in school publicity materials can increase pupil motivation and help parents and the local community identify and celebrate the school's achievements.

We only use images that the Head Teacher and Governing Body consider suitable and which appropriately represent the range of activities the school provides and the values it adheres to. No images will be used which could be considered to put any child at increased risk.

Through this policy we aim to respect young people's and parents' rights of privacy and minimise the risks to which young people can be exposed through the misuse of images. The policy takes account of both data protection and child protection issues.

Data protection

Photographs and video images of pupils and staff are classed as personal data under the terms of the Data Protection Act 1998. We will not use images of identifiable individuals for school publicity purposes without the consent of either the individual themselves or, in the case of pupils, their parent, guardian or carer. General consent will be gained from parents on the attached consent form (attached to this policy) when sent with the contact form on an annual basis. Specific consent by phone is obtained if children's names and photographs are to be used in newspapers.

In seeking consent, we will ensure that parents are clear why we are using a child's image and what we are using it for. (See Appendix A for school consent form)

General consent is requested through the completion of the Child Photograph Consent Form/Website Consent Form. This is completed as part of the school's admission procedures.

Specific consent may be sought from parents for particular projects involving the taking of children's photographs. In seeking specific consent, we will ensure that parents are clear why we are using a child's image, what we are using it for and who might want to look at the pictures. Any specific consent form will make clear the period of time for which consent applies.

All original images will be stored securely and used only by those who are authorised to do so. We will not re-use images of children after they have left the school; these images will be destroyed.

Child protection

We will only use images of children in suitable dress. The Head Teacher and Governing Body will decide if images of some activities – such as sports or arts – are suitable without presenting risk of potential misuse.

Any evidence of the use of inappropriate images, or the misuse of images, will be reported to the school's child protection designated teacher, the LEA, Social Services and/or the police as appropriate.

Individual pupils will not be named in conjunction with their image unless parental consent received and we will never use an image of a child who is subject to a court order.

School Website

We will adopt the same principles as outlined above when publishing images on the internet as we would for any other kind of publication or publicity material. However, the school recognises that there is no control over who may view images, and consequently a greater risk of misuse of images, via the internet. We will therefore give specific

consideration to the suitability of images for use on the school's website.

Images, and accompanying details, will only be used in line with government guidance.

Webcams and mobile phones

1. The school recognises that webcams and mobile phones can be used to take images without people's knowledge. If any webcam is in use, the area will be signposted so that people know the webcam is there before they enter that area.

Misuse of mobile phones that can take and transmit images will be regarded as a breach of school discipline and dealt with accordingly. Such phones will not be allowed in areas where children are changing and must not be used to take children's photographs in school at any time.

All staff sign to say that they have read the 'Code of Conduct' every year. This clearly states the rules regarding the use of mobile phones, the storing of photographs and the rules surrounding social media and the internet. No photographs of children in school should be stored on a personal device.

External photographers and events

If the school invites or permits an external photographer to take photographs within school, we will:

- Provide a clear brief for the photographer about what is considered appropriate in terms of content and behaviour
- Issue the photographer with identification which must be worn at all times
- Let children and parents know that a photographer will be in attendance at an event and ensure they consent to both the taking and publication of films or photographs
- Not allow unsupervised access to children or one-to-one photo sessions at events.

The same conditions will apply to filming or video-recording of events.

Photographs taken by journalists are exempt from the Data Protection Act as newspapers are subject to strict guidelines governing the press. Newspaper photographers may only take photos of children with permission from the school. If asked, the school will provide names and ages of children for publication in newspapers. No specific address and no other contact details will be supplied. The general consent requested on the Admission Form includes permission for newspaper photographs. However, wherever possible and practicable, we will inform parents before allowing journalists to take photographs of pupils. Parents may then request that their child not be included.

Parents and Carers

It is the policy of the School to allow Parents and Carers to take photographs and videos at school events. Those wishing to record such events must inform the school. This applies to cameras, videos and mobile phones. Parents are reminded that the pictures are for their personal use only and that they should not be shared online.

Images taken by Children

The school encourages children to take photographs and videos of each other as a way of recording events. This may take place in school, on school trips or on residential visits.

The use of cameras within school, on trips or visits is part of the pleasure and the learning in the experience.

There is no reason why pupils should not be allowed to take photographs so long as anyone photographing respects the privacy of the person being photographed.
This is seen as part of the school's code of behaviour.

Infringement of this respect of privacy will be dealt with in the same way as any other breach of school discipline.

Seesaw

Seesaw is an app that is used by staff to communicate with parents. Pictures and videos can be shared to enable parents and carers to be more involved in their child's education. Parents give consent for the app to be used and are responsible for downloading a QR code to gain access. Children who cannot have photographs taken are not included on group photographs and/or may only have pictures of their work sent home. The comments function has been removed as has the function to enable parents to share photographs or publish them online.

A4 – The Lanes GDPR Information Letter

The Lanes PRIMARY SCHOOL

Cator Lane, Chilwell, Nottingham NG9 4BB
Tel: 0115 9138558 / 9138562
Meadow Lane Site Tel: 0115 9190644
Website: www.thelanes.notts.sch.uk
Email: office@thelanes.notts.sch.uk
Head Teacher: Mrs J Revill
Deputy Heads: Mrs M Brown and Miss A Hodkin

Summer 2020

Dear Parents/Carers

As you may be aware, new legislation around data protection came into force in 2018. The legislation is entitled *The General Data Protection Regulation* (GDPR). While it is broadly similar to previous regulations, it has meant changes to how schools store and use personal data and it will strengthen individuals' rights in relation to their personal data.

All parents and carers are now being asked to provide specific consent for the use of their child's image. Individuals must now specifically opt-in to allow images to be used for purposes such as the website, newsletters or press releases.

We must ask you to choose Yes or No for every option and, **should you choose No for all options we will still require you to return your form to the school**. Clearly we wish to celebrate student's achievements as often as we can, share their fun on a school trip, or allow families to see images from school activities and productions. We encourage an inclusive environment at The Lanes, but do understand that the final decision over photo consent rests with parents/carers.

The consent form remains in place for the duration of your child's time at The Lanes Primary School. However, if you would like to change your consent levels at any stage please contact the school office to update your form which is held on file.

Please can you complete and return the form overleaf by Monday 7 September 2020 at the latest, so that we have this information for the new academic year.

Yours sincerely

Joanne Revill
Head Teacher

A5 – The Lanes GDPR Form

GDPR Photographic and Video Consent Form

Name of Pupil: .....

Please note: The information on this form will be relevant throughout your child's education at The Lanes Primary School Please tick either Yes or No for each of the statements below:

	Website and external publications:	**YES**	**NO**
1	**I consent to the use of my child's image on The Lanes website.** For example, to celebrate their achievements, taking part in an assembly or class activities, taking part in sporting events or school production.		
2	**I consent to the release of my child's name for publication, with or without an accompanying image such that they may be identified as an individual or part of a small group.** This may include the local press or media.		
3	**I consent to the use of my child's work on the school website.** For example a poster designed for an event, an outstanding piece of writing or art work.		
4	**I consent to the use of my child's image (without their name) in the school prospectus and in other printed publications/displays that we produce for promotional purposes.** An example could be a photograph of them in a general classroom scene with other students/staff.		
5	**I consent to the use of my child's image in any school or class yearbook or other mementos on leaving school.**		
	Photos/Videos in and around school:		
6	**I consent to the use of my child's image in a display in school, which includes our information screens that may be viewed by visitors to the school.** An example may include a display in the school entrance or on the display screen in the playground. All digital images will be destroyed two years after your child has left The Lanes Primary School.		
7	**I consent to the release of my child's name, with or without an accompanying image such that they may be identified as an individual or part of a small group.** This may include school displays and newsletters and the **Seesaw app.**		
8	**I consent to my child being photographed for school group photos that may be purchased by other families who have children within the photo.** For example, a class photo, leaver's photo or school produced dvd collection of photos.		
9	**I consent for a professional photographer appointed and approved by the school to photograph my child and release the images to our family for sale.** Please note: the photographer would have possession of the photos on their equipment, not school equipment. A copy of all these school photographs is kept for one year in school and then securely destroyed.		

- Please note 'image' refers to photographic & video recording.
- Please ensure you have answered Yes or No to **all** questions then return the form to school.

Signed.....(parent/carer)

A6 – The Lanes Home School Agreement

Home School Agreement

The Lanes Primary School

Head teacher: Mrs Joanne Revill

A message to parents and carers from the Head teacher and the Chair of Governors.

Welcome to The Lanes Primary School. We firmly believe that a close partnership between home and school is vital to help children and young people get the best from their education.

Home-school agreements are part of every school's partnership with parents. This agreement enables parents, teachers and pupils to make a clear commitment to working together.

The agreement makes clear what is expected of teachers, parents and carers to ensure pupils will be able to work hard and be happy, safe and successful at school. We hope that it will also help parents and carers to take an active role in their child's education at The Lanes Primary school.

We are determined to give each pupil every chance to do well. We look forward to a strong partnership with home to give your child the best possible start.

Please sign and return this form to your child's class teacher by Friday 14 January 2022

Child's name _____ **Class** _____

I/We the parents/carers will aim to:

Ensure my child is prepared for the day ahead by having had adequate rest and breakfast.

Ensure my child has excellent attendance - avoiding taking holidays during term time and will inform the school promptly on the day of any absence.

Ensure that my child gets to school promptly and properly equipped including the agreed school uniform, water bottle and PE kit.

Make the school aware of any concerns or problems that might affect my child's work or behaviour – avoiding the use of social media to address these.

Support the school's policies and approach to behaviour.

Support and ensure my child completes any homework / home learning tasks. Support my child's learning further by practising spellings set in school.

Attend parent's evenings / discussions about my child's progress and other key school events.

Ensure that I read with and listen to my child read as often as possible at home.

Signed ..... (parent/carer)

The pupils

To help me do well at school, I will do my best to:

- Always do my best at my learning
- Work hard towards achieving my targets
- Talk at home about what I learn at school
- Do all my home activities and homework
- Not miss school and always try to be on time
- Wear my school uniform
- Take responsibility for all my own belongings and respect the belongings of others.
- Behave well and keep the school rules.
- Be polite and helpful to other pupils and adults
- Always try to enjoy school and help other children to do the same
- Talk to my teacher if I am unhappy or need help.
- Read at least 4 times every week.
- Take newsletters and other information home promptly.
- Follow the e safety rules in school.

Signed _____**Pupil**

Parent/Carers consent form and e-safety rules

All pupils will have access to the school's computer facilities including the internet as an essential part of learning, as required by the National Curriculum.

As the parent or legal guardian of the above pupil, I grant permission for my son/daughter to use the internet, school e-mail system, learning platform and other ICT facilities at School.

I know that my son/daughter knows the e safety rules in school.

We have discussed these rules and they agree to follow the rules to support the safe and responsible use of ICT at School.

I accept that the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies, but I understand that they will take every reasonable precaution to keep pupils safe and to prevent pupils accessing inappropriate materials.

The school has an educationally filtered service, restricted access email and provides age appropriate teaching around internet use and e-safety issues.

I will support the school by promoting safe use of the internet and digital technology at home and will inform the school if I have any concerns over my child's e-safety.

Signed _____ Parent / Carer

The School.

We will:

Value and respect each child as an individual.

Care for each child's safety and happiness

Recognise and praise progress and achievement

Address the individual needs of each child by providing a broad and balanced curriculum.

Encourage all children to reach their full potential in a supportive learning environment.

Inform parents of their child's progress and learning through regular contact.

Encourage all children to take care of their surroundings and others around them.

Encourage your child to adopt a healthy lifestyle

Promote high standards of work and behaviour through building good relationships and developing a sense of responsibility.

Contact you as soon as possible if we have worries about your child's work or behaviour or attendance/punctuality.

Provide a range of in school and after school activities designed to enrich your child's experience

Signed J. Lewis ***Head teacher***

Our Internet Rules

We use the Internet safely to help us learn.

We learn how to use the Internet.

We can send and open messages with an adult.

We only tell people our first name.

We do not tell anyone our password.

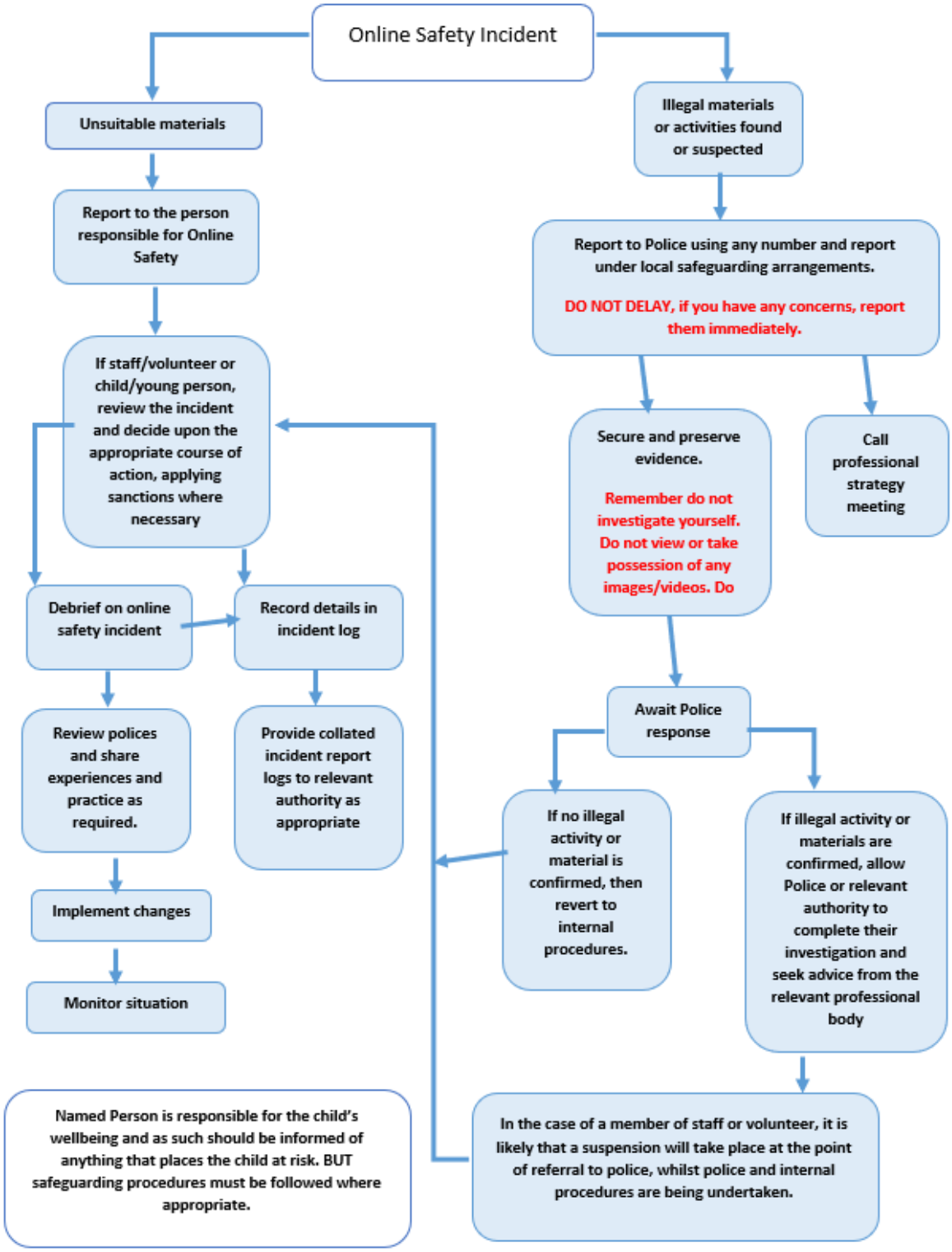
We know who to ask for help.

If we see something we do not like we know what to do.

We know that it is important to follow the rules.

We are able to look after each other by using our safe Internet.

A7 Responding to incidents of misuse – flow chart



A8 Record of reviewing devices/internet sites (responding to incidents of misuse)

Group: .....

Date: .....

Reason for investigation: .....

.....

.....

Details of first reviewing person

Name: .....

Position: .....

Signature: .....

Details of second reviewing person

Name: .....

Position: .....

Signature: .....

Name and location of computer used for review (for web sites)

.....

.....

Web site(s) address/device	Reason for concern

Conclusion and Action proposed or taken

A9 Reporting Log

Group: .....

Date	Time	Incident	Action Taken		Incident Reported By	Signature
			What?	By Whom?		