E-Safety Policy

Last Revised: August 2023

Policy Owner: Head of ICT

Date of next review: ________August 2024 _______

Signed: ____________Ed Currie ___________________ Date: ______1.8.23_________

Printed: _________Mr Ed Currie ______________________

Chair of Governors

Signed: _______________Andrew Rudkin _________________ Date: ________1.8.23_______

Printed: __________Mr Andrew Rudkin _____________________

(Headmaster)

Policy Statement

This is a whole school policy and applies to all members of Lyndhurst School including Early Years (Reception – Nursery), where the Early Years Foundation Stage (EYFS) Framework is followed. We use the Development Matters (2021) as a guide for planning.

This E-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 Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off Lyndhurst School site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other online safety incidents covered by this policy, which may take place outside of Lyndhurst School, but is linked to membership of Lyndhurst School. The 2011 Education Act increased these powers regarding the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy

Lyndhurst 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.

Associated Policies and Documents

- Safeguarding and Child Protection Policy
- Behaviour Policy
- Anti-Bullying Policy
- ICT Acceptable Use Agreements (Pupils, Parents, Staff, Visitors)
- Data Protection Policy
- Privacy Notice
- Internet filtering Policy
- Keeping Children Safe in Education (2022)

Support

Ictsupprt@ and activeit@ can be used for any ICT support

Or please contact the school bursar – c.hughes@lyndhurstschool.co.uk

Roles and Responsibilities

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 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 may be delegated to the E- Safety Lead.

- The headteacher and (at least) another member of 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[1].
- The headteacher/senior leaders are responsible for ensuring that the Online Safety Lead, 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 the Online Safety Lead.

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 E-Safety Policy and for reviewing the effectiveness of the policy.

This review will be carried out by the Chair of Governors and the Safeguarding Governor who will receive regular information about online safety incidents and monitoring reports. A member of the governing body will take on the role of E-Safety Governor to include:

- regular meetings with the E-Safety Lead
- 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.

E- Safety Lead

The E- Safety Lead will:

[1] See flow chart on dealing with online safety incidents in ‘Responding to incidents of misuse’ and relevant local authority/MAT/ HR/other relevant body disciplinary procedures.

- lead the Online Safety Group
- work closely on a day-to-day basis with the Designated Safeguarding Lead (DSL), where these roles are not combined.
- 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, mapped, 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 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, pastoral 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.
- attend relevant governing body meetings/groups.
- report regularly to headteacher/senior leadership team.
- liaises with the local authority/MAT/relevant body.

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 [2]
- access to illegal/inappropriate materials
- inappropriate online contact with adults/strangers
- potential or actual incidents of grooming
- online bullying

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 Online Safety Lead 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.

[2] See ‘Personal data policy’.

Network manager/technical staff

The network manager/technical staff (or local authority/MAT/technology provider) is responsible for ensuring that:

- they are aware of and follow the school Online Safety Policy and Technical Security 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/MAT or other relevant body.
- 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 online safety lead 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.

Children

- 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

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
- sharing an online safety newsletter termly
- 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 appropriate.

Community users / Visitors

Community users who access school systems/website/learning platform as part of the wider school provision will be expected to sign a community user AUA before being provided with access to school systems.

Aims and Ethos

E-Safety Policy

The school E-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 normal communication channels.
- is published on the school website.

Education – Children

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety/digital literacy is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

E-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 will be provided as part of Computing/PHSE/other lessons and should be regularly revisited.
- Key online safety messages will be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities.
- Pupils will be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils will be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Pupils will be helped to understand the need for the pupil acceptable use agreement and encouraged to adopt safe and responsible use both within and outside the 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 pupils 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 pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

Education – Parents/carers

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.

Lyndhurst School will therefore seek to provide information and awareness to parents and carers through:

- National Online Safety Training
- Curriculum activities
- Letters, newsletters,
- Parents/carers evenings/sessions

- High profile events/campaigns e.g. Safer Internet Day
- Reference to the relevant web sites/publications *e.g.* swgfl.org.uk, www.saferinternet.org.uk/, http://www.childnet.com/parents-and-carers

Education & Training – Staff/Volunteers

It is essential that all staff 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 training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand Lyndhurst School online safety policy and acceptable use agreements.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- The Online Safety Lead will receive regular updates through attendance at external training events 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/training sessions.
- The Online Safety Lead will provide advice/guidance/training to individuals as required.

Training – Governors

Governors should take part in online safety training/awareness sessions, with importance for those who are members of any group involved in technology/online safety/health and safety /safeguarding. This will be via National Online Safety.

Technical – infrastructure/equipment, filtering and monitoring

Lyndhurst School will be responsible via the outsourced support company, Perfect Fit, for ensuring that the infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- Lyndhurst School technical systems will be managed in ways that ensure that it meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of Lyndhurst School technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to Lyndhurst School technical systems and devices.

- All users will be provided with a username and secure password by the E-Safety Lead, who will keep an up-to-date record of users and their usernames. Users are responsible for the security of their username and password.
- The "master/administrator" passwords for Lyndhurst School systems, used by the IT Support company must also be available to the Headmaster or online safety lead and kept in a secure place.
- The IT Support company is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation Child Abuse Image Content (CAIC) list. Content lists are regularly updated, and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes (see appendix for more details)
- Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- Lyndhurst School has provided enhanced/differentiated user-level filtering.
- The outsourced IT support company, Perfect Fit, regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement.
- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices, etc. 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 devices are protected by up-to-date virus software.

<u>Personal devices:</u>

- Staff and visitors can use personal mobile devices in school away from the children in the staff workroom, staffroom and individual offices. The children are only allowed to use personal devices when they have specific permissions to support them with their learning/medical reasons.
- The use of personal devices is restricted to these spaces and at no time should they be used in the presence of children.
- Personal devices must be locked away from others.
- Staff can take personal devices on school trips, in cases of emergency in order to contact the main school and also for school business such as during emergency evacuation of premises. These staff members are indicated on the Emergency Evacuation Procedure Plan.
- No technical support is available for the use of personal devices.
- Data Protection Policy applies to the use of personal devices.
- The school has a right to take, examine and search users' devices if they are used on the school premises in the case of misuse.

- At no time should an individual take or store or use images for school on their personal devices.
- The school cannot be held liable for loss/damage or malfunction of personal devices following access to the network.
- All personal devices must be identifiable by others in school.
- Visitors will be informed about school requirements with regards to the use personal devices as they enter the school.
- The education of the safe and responsible use of mobile devices is included in the school online safety education.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and children 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. When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. They should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

- Written permission from parents or carers will be obtained as part of the admission forms.
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at Lyndhurst School events for their own personal use (as such use is 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 pupils in the digital/video images.
- Staff and volunteers can take digital/video images to support educational aims, but must follow Lyndhurst School policies concerning the sharing, distribution and publication of those images. Those images should only be taken on Lyndhurst School equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or Lyndhurst School into disrepute.
- Children must not take, use, share, publish or distribute images of others without their permission.

- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

Data Protection

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

Lyndhurst School:

- it has a Data Protection Policy.
- it implements the data protection principles and can demonstrate that it does so through use of policies, notices and records.
- it has paid the appropriate fee Information Commissioner's Office (ICO) and included details of the Data Protection Officer (DPO).
- it has appointed an appropriate Data Protection Officer (DPO) who has a high level of understanding of data protection law and is free from any conflict of interest.
- it has an 'information asset register' in place and knows exactly what personal data it holds, where this data is held, why and which member of staff has responsibility for managing it.
- the information asset register records the lawful basis for processing personal data (including, where relevant, how consent was obtained and refreshed). Where special category data is processed, an additional lawful basis will have also been recorded.
- it will hold only the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for. The school should develop and implement a 'retention policy" to ensure there are clear and understood policies and routines for the deletion and disposal of data to support this. Personal data held must be accurate and up to date where this is necessary for the purpose it is processed for. Have systems in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals.
- it provides staff, parents, volunteers and older children with information about how the Lyndhurst School looks after their data and what their rights are in a clear Privacy Notice
- procedures are in place to deal with the individual rights of the data subject, e.g. one of the 8 data subject rights applicable is that of Subject Access which enables an individual to see to have a copy of the personal data held about them (subject to certain exceptions which may apply).
- Data Protection Impact Assessments (DPIA) are carried out where necessary. For example, to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier (this

may also require ensuring that data processing clauses are included in the supply contract or as an addendum)

- IT system security is ensured and regularly checked. Patches and other security essential updates are applied promptly to protect the personal data on the systems. Administrative systems are securely ring fenced from systems accessible in the classroom/to learners.
- it has undertaken appropriate due diligence and has required data processing clauses in contracts in place with any data processors where personal data is processed.
- it understands how to share data lawfully and safely with other relevant data controllers.
- It reports and breaches to the Information Commissioner within 72hrs of becoming aware of the breach in accordance with UK data protection 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.
- all staff receive data protection training at induction and appropriate refresher training thereafter. Staff undertaking 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 must be encrypted, and password protected.
- device must be password protected. (be sure to select devices that can be protected in this way)
- device must be protected by up-to-date virus and malware checking software.
- data must be securely deleted from the device, in line with Lyndhurst 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 understands their rights and know how to handle a request whether verbal or written. Know who to pass it to in the school.
- where personal data is stored or transferred on mobile or other devices (including USBs) these must be encrypted and password protected.
- will not transfer any Lyndhurst School personal data to personal devices except as in line with school policy.
- access personal data sources and records 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.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning.

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

- The official Lyndhurst School email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and children should therefore use only the Lyndhurst School email service to communicate with others when in school, or on Lyndhurst School systems (e.g. by remote access).
- Users must immediately report to the nominated person – in accordance with the Lyndhurst 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.
- Any digital communication between staff and children or parents/carers (email, social media, chat, blogs) must be professional in tone and content. These communications may only take place on official (monitored) Lyndhurst School systems. Personal email addresses, text messaging or social media must not be used for these communications.
- All children will be provided with individual Lyndhurst School email addresses for educational use.
- Children are taught about online safety issues, such as the risks attached to the sharing of personal details. They are also taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the Lyndhurst School website and only official email addresses should be used to identify members of staff.
- Employees must not send abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory, pornographic or otherwise inappropriate emails from equipment provided for work by Lyndhurst School. Please also see section relating to social media in relation to sites accessed for personal use on their own devices.
- Employees should adopt a professional tone and observe appropriate etiquette when communicating by email.
- Employees should not send out sensitive data through email unless the information is encrypted, or password protected.
- Employees should remember that emails can be used in legal proceedings and may be required in response to Subject Access Requests, and that even deleted emails may remain on the system and are capable of being retrieved.

Employees must not:

- Use their own personal email account to send or receive email for the purposes of Lyndhurst School business; only the email account provided for employees should be used.

- Send, forward or read private emails at work which they would not want a third party to read.
- Send or forward chain mail, junk mail, cartoons, jokes or gossip.
- Send messages from another person's email address (unless authorised) or under an assumed name.
- Open unsolicited emails or any attachments they may include.
- Not respond to "Phishing" emails, including any requests for information they include – these are created to look official, from a bank or other reputable organisation. They can contain dangerous links or claim that there has been a security breach. These links are usually directed to fake sites that collect personal information, often used to steal money or other sensitive data. Reputable organisations will never ask for details in this manner. Lyndhurst School is not responsible for any personal loss/damage caused as a result of clicking on such links.

Employees should also carefully consider whether it is necessary to send an email and consider the workload impact of the recipient/whether a phone call would be more appropriate.

Social Media Use

Lyndhurst School has a duty of care to provide a safe learning environment for children and staff. Schools could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render Lyndhurst School liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

Lyndhurst School provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published.
- Training is provided including ICT acceptable use agreement; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions.
- Risk assessment, including legal risk.

Lyndhurst School staff should ensure that:

- No reference should be made in social media to children, parents/carers or Lyndhurst 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 Lyndhurst School.
- Security settings on personal social media profiles are regularly checked to minimise the risk of loss of personal information.

When official Lyndhurst School social media accounts are established there:

- Is a process for approval by the Headteacher

- The school uses an external consultant to monitor our social media. Conquest Consultancy.
- Are clear processes for the administration and monitoring of these accounts by the Headteacher and the Marketing and Admissions Lead who both own the administrative rights.
- Is a code of behaviour for users of the accounts? Please see Staff Code of Conduct
- Are systems for reporting and dealing with abuse and misuse. Our social media provider uses digital listening software that monitors the social media space so that any harmful content targeted at the school can be quickly removed. In addition, any negative conversations can be closed down very quickly to protect the brand's reputation.
- Is an understanding of how incidents may be dealt with under Lyndhurst School disciplinary procedures in the school's Code of Conduct.

Personal Use:

- Personal communications are those made via a personal social media account. In all cases, where a personal account is used which associates itself with the Lyndhurst School or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the Lyndhurst 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 Lyndhurst School permits reasonable and appropriate access to private social media sites.

Monitoring of Public social media:

- As part of active social media engagement, it is considered good practice to 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.

Lyndhurst School's use of social media for professional purposes will be checked regularly by the senior risk officer to ensure compliance with the school policies.

Dealing with unsuitable/inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school/academy context, either because of the age of the users or the nature of those activities.

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in/or outside the school when using school equipment or systems.

The school policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	

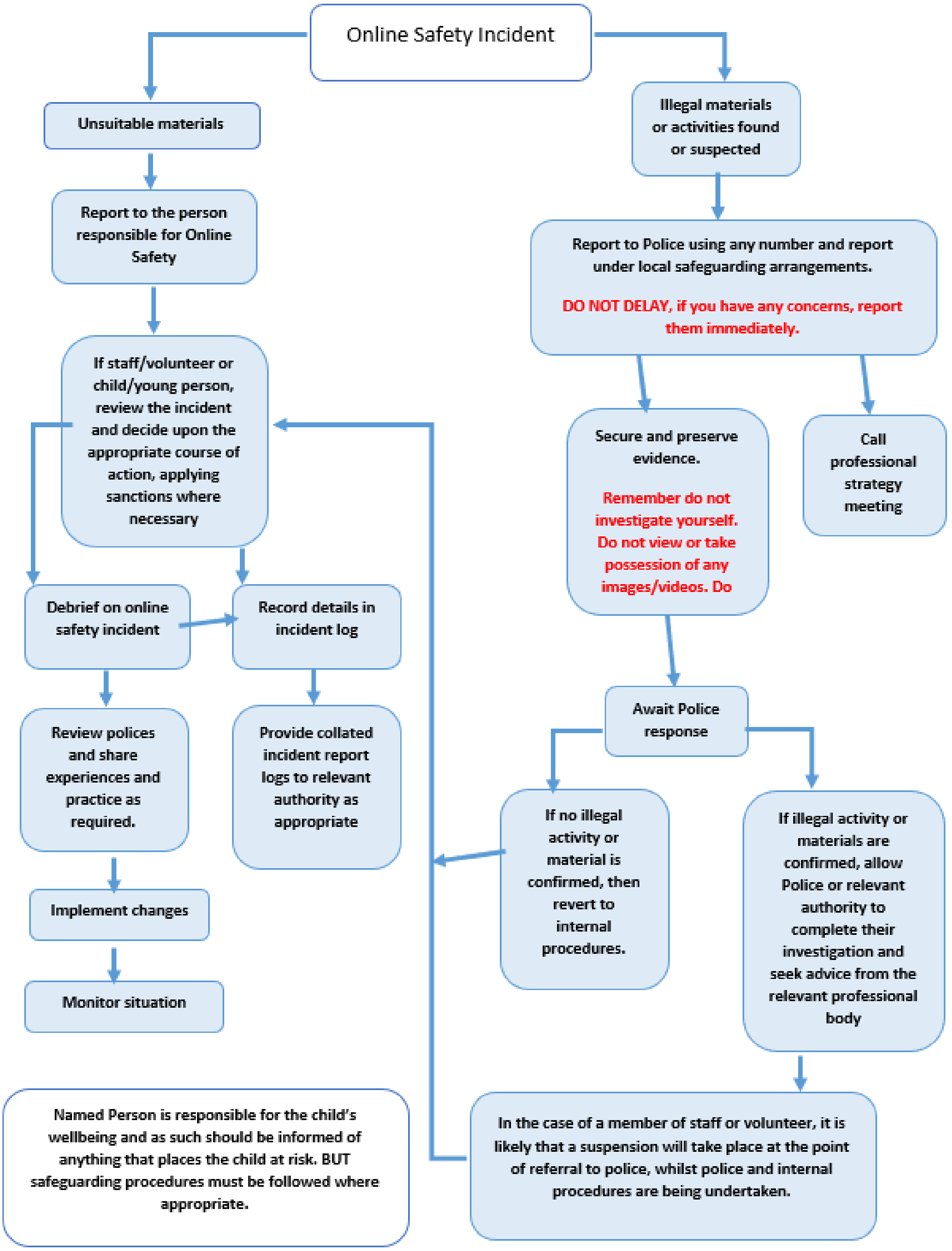
Activities that might be classed as cyber-crime under the Computer Misuse Act: • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices. • Using penetration testing equipment (without relevant permission)					X
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school/academy				X	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)				X	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)				X	
Using school systems to run a private business				X	
Infringing copyright				X	
On-line gaming (educational)			X		
On-line gaming (non-educational)				X	
On-line gambling					X
On-line shopping/commerce			X		
File sharing			X		
Use of social media			X		
Use of messaging apps			X		
Use of video broadcasting e.g. YouTube			X		

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see “User Actions” above).

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right-hand side of the Flowchart (below) for responding to online safety incidents and report immediately to the police.



Online Safety Incident

Unsuitable materials

Report to the person responsible for Online Safety

If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary

Debrief on online safety incident

Record details in incident log

Review polices and share experiences and practice as required.

Provide collated incident report logs to relevant authority as appropriate

Implement changes

Monitor situation

Illegal materials or activities found or suspected

Report to Police using any number and report under local safeguarding arrangements.

DO NOT DELAY, if you have any concerns, report them immediately.

Secure and preserve evidence.

Remember do not investigate yourself. Do not view or take possession of any images/videos. Do

Call professional strategy meeting

Await Police response

If no illegal activity or material is confirmed, then revert to internal procedures.

If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body

In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.

Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by a child and if necessary, can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should 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 (except in the case of images of child sexual abuse – see below)
- 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
    - Police involvement and/or action
- If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - incidents of ‘grooming’ behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism
    - offences under the Computer Misuse Act (see User Actions chart above)
    - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

School actions & sanctions

It is more likely that Lyndhurst 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 using the below.

Children Actions/Sanctions

Students/Pupils Incidents	Refer to Headteacher/	Refer to Police	Refer to technical support staff for action re filtering/security	Inform parents/carers	Removal of network/internet access rights	Warning	Further sanction e.g. exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).	X	X	X	X	X	X	
Unauthorised use of non-educational sites during lessons	X		X	X	X	X	X
Unauthorised/inappropriate use of mobile phone/digital camera/another mobile device	X			X	X	X	X
Unauthorised/inappropriate use of social media/ messaging apps/personal email	X			X	X	X	X
Unauthorised downloading or uploading of files	X		X	X	X	X	X
Allowing others to access school network by sharing username & passwords	X		X	X	X	X	X
Attempting to access or accessing the school network, using another children's account	X		X	X	X	X	X
Attempting to access or accessing the school network, using the account of a member of staff	X		X	X	X	X	X
Corrupting or destroying the data of other users	X		X	X	X	X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X		X	X	X	X	X
Continued infringements of the above, following previous warnings or sanctions	X		X	X	X	X	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X		X	X	X	X	X
Using proxy sites or other means to subvert the school's filtering system	X		X	X	X	X	X
Accidentally accessing offensive or pornographic material & failing to report the incident	X	X	X	X	X	X	X
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X	X	X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X		X	X	X	X	X

Staff Incidents	Refer to Headteacher	Refer to Governors & Directors	Refer to Police	Refer to Technical Support Staff for action re	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).	X	X	X	X	X	X	X
Inappropriate personal use of the internet/social media/personal email	X	X		X	X	X	X
Unauthorised downloading or uploading of files	X	X		X	X	X	X
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X	X		X	X	X	X
Careless use of personal data e.g. holding or transferring data in an insecure manner	X	X		X	X	X	X
Deliberate actions to breach data protection or network security rules	X	X		X	X	X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X		X	X	X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X		X	X	X	X
Using personal email/social networking/instant messaging/text messaging to carrying out digital communications with children	X	X		X	X	X	X
Actions which could compromise the staff member's professional standing	X	X		X	X	X	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X		X	X	X	X
Using proxy sites or other means to subvert the school's filtering system	X	X		X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X	X	X	X	X
Deliberately accessing or trying to access offensive or pornographic material							
Breaching copyright or licensing regulations	X	X	X	X	X	X	X
Continued infringements of the above, following previous warnings or sanctions	X	X		X	X	X	X