Online Safety Policy

Presented to the board on	8th September 2021
To be ratified following comments by	24th September 2021

Contents

1. Policy Aims

2. Policy Scope

    2.2 Links with other policies and practices

3. Monitoring and Review

4. Roles and Responsibilities

    4.1 The leadership and management team

    4.2 The Designated Safeguarding Lead

    4.3 Members of staff

    4.4 Staff who manage the technical environment

    4.5 Pupils

    4.6 Parents

5. Education and Engagement Approaches

    5.1 Education and engagement with pupils

    5.2 Vulnerable Pupils

    5.3 Training and engagement with staff

    5.4 Awareness and engagement with parents

6. Reducing Online Risks

7. Safer Use of Technology

    7.1 Classroom Use

    7.2 Managing Internet Access

    7.3 Filtering and Monitoring

    7.4 Managing Personal Data Online

7.5 Security and Management of Information Systems

7.6 Managing the Safety of the Website

7.7 Publishing Images and Videos Online

7.8 Managing Email

7.9 Educational use of Videoconferencing and/or Webcams

7.10 Management of Learning Platforms

7.11 Management of Applications (apps) used to Record Pupils Progress

8. Social Media

8.1 Expectations

8.2 Staff Personal Use of Social Media

8.3 Pupils Personal Use of Social Media

8.4 Official Use of Social Media

9. Use of Personal Devices and Mobile Phones

9.1 Expectations

9.2 Staff Use of Personal Devices and Mobile Phones

9.3 Pupils Use of Personal Devices and Mobile Phones

9.4 Visitors' Use of Personal Devices and Mobile Phones

9.5 Officially provided mobile phones and devices

10. Responding to Online Safety Incidents and Concerns

10.1 Concerns about Pupil Welfare

10.2 Staff Misuse

11. Procedures for Responding to Specific Online Incidents or Concerns

11.1 Online Sexual Violence and Sexual Harassment between Children

11.2 Youth Produced Sexual Imagery or "Sexting"

11.3 Online Child Sexual Abuse and Exploitation

11.4 Indecent Images of Children (IIOC)

11.5 Cyberbullying

11.6 Online Hate

11.7 Online Radicalisation and Extremism

12. Useful Links for Educational Settings

Appendix A - Acceptable Use Policy

1. Policy Aims

The purpose of East London Science School online safety policy is to:

- Safeguard and protect all members of East London Science School community online.
- Identify approaches to educate and raise awareness of online safety throughout the community.
- Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns.

East London Science School identifies that the issues classified within online safety are considerable, but can be broadly categorised into three areas of risk:

- Content: being exposed to illegal, inappropriate or harmful material
- Contact: being subjected to harmful online interaction with other users
- Conduct: personal online behaviour that increases the likelihood of, or causes, harm.

2. Policy Scope

East London Science School believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all pupils and staff are protected from potential harm online. ELSS identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life. We believe that pupils should be empowered to build resilience and to develop strategies to manage and respond to risk online.

This policy applies to all staff including the governing body, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the setting (collectively referred to as "staff" in this policy) as well as pupils, parents and carers. This policy applies to all access to the internet and use of technology, including personal devices, or where pupils, staff or other individuals have been provided with setting issued devices for use off-site, such as a work laptops, tablets or mobile phones.

2.2 Links with other policies and practices

This policy links with several other policies (but not limited to):

- Scholarly Behaviour Policy
- Anti-bullying policy
- Code of conduct and the Staff Handbook
- Safeguarding and Child protection policy
- Teaching and Learning Policy

3. Monitoring and Review

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

4. Roles and Responsibilities

The Designated Safeguarding Lead (DSL) Jennifer Copestake has lead responsibility for online safety. Whilst activities of the designated safeguarding lead may be delegated to appropriately trained deputies, the ultimate lead responsibility for safeguarding and child protection remains with the DSL. ELSS recognises that all members of the community have important roles and responsibilities to play with regards to online safety. Bright Adjushi, IT manager, also has a lead role in ensuring the online safety of the school community.

4.1 The leadership and management team will:

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.

- Ensure there are appropriate and up-to-date policies regarding online safety; including a staff code of conduct and handbook, which covers acceptable use of technology.
- Ensure that suitable and appropriate filtering and monitoring systems are in place and work with technical staff to monitor the safety and security of our systems and networks; as schools increasingly work online, it is essential that children are safe guarded from potentially harmful and inappropriate online material (including when they are online at home).
- Ensure that online safety is embedded within our curriculum, which enables all pupils to develop an age-appropriate understanding of online safety.
- Support the DSL and any deputies by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.
- Ensure there are robust reporting channels for the community to access regarding online safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology.
- Audit and evaluate online safety practice to identify strengths and areas for improvement.

4.2 The Designated Safeguarding Lead (DSL) will:

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

- Work with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input.
- Meet regularly termly with the governor with a lead responsibility for safeguarding and/or online safety.

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

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

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

- Provide technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Implement appropriate security measures to ensure that the settings IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensure that our filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- Report any filtering breaches to the DSL (or deputy DSLs) and leadership team, as well as, the settings Internet Service Provider or other services, as appropriate.
- Ensure that any safeguarding concerns, identified through monitoring or filtering breaches are reported to the DSL (or deputy DSLs), in accordance with the safeguarding procedures.

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

- Engage in age appropriate online safety education opportunities.
- Contribute to the development of online safety policies.
- Read and adhere to the acceptable use policies.
- Respect the feelings and rights of others both on and offline.
- Take responsibility for keeping themselves and others safe online.

- Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues.

4.6 It is the responsibility of parents and carers to:

- Read the policy and encourage their children to adhere to them.
- Support our online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home.
- Role model safe and appropriate use of technology and social media.
- Abide by the acceptable use policies.
- Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the setting, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Contribute to the development of the online safety policies.
- Use our systems, such as learning platforms, and other network resources, safely and appropriately.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

5. Education and Engagement Approaches

5.1 Education and engagement with pupils

The school will establish and embed a progressive online safety curriculum to raise awareness and promote safe and responsible online behaviour at school and at home amongst pupils by:

- Ensuring education regarding safe and responsible use precedes internet access.
- Including online safety in relevant programmes of study.
- Reinforcing online safety messages whenever technology or the internet is in use.
- Educating pupils in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
- Teaching pupils to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

ELSS will support pupils to read and understand the acceptable use policies in a way which suits their age and ability by:

- Displaying acceptable use posters in key rooms with internet access.
- Informing pupils that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
- Providing online safety education and training as part of the transition programme across the key stages and when moving between establishments.
- Using support, such as external visitors, where appropriate, to complement and support our internal online safety education approaches.

5.2 Vulnerable Pupils

ELSS recognises that some pupils are more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss. When implementing an appropriate online safety policy and curriculum we will seek input from specialist staff as appropriate, including the SENCO, Designated Teacher for LAC and other appropriate staff.

5.3 Training and engagement with staff

We will:

- Provide and discuss the online safety policy and procedures with all members of staff as part of induction.
- Provide up-to-date and appropriate online safety training for all staff on a regular basis, with at least annual updates. This will be done through stand-alone sessions or through drip feeding with small sessions/ daily briefing reminders.
- This will cover the potential risks posed to pupils (Content, Contact and Conduct) as well as our professional practice expectations.
- Recognise the expertise staff build by undertaking safeguarding training and managing safeguarding concerns and provide opportunities for staff to contribute to and shape online safety policies and procedures.
- Make staff aware that our IT systems are monitored, and that activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices.
- Make staff aware that their online conduct outside of the setting, including personal use of social media, could have an impact on their professional role and reputation.
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the pupils.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting pupils, colleagues or other members of the community.

5.4 Awareness and engagement with parents and carers

East London Science School recognises that parents and carers have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies. We will build a partnership approach to online safety with parents and carers by:

- Providing information and guidance on online safety in a variety of formats.

- This will include offering specific online safety awareness training and highlighting online safety at other events such as parent evenings and transition events as well as on our social media platforms.
- Drawing their attention to the online safety policy and expectations on our website.
- Requesting that they read online safety information as part of joining our community.
- Requiring them to read our acceptable use policies and discuss the implications with their children.

6. Reducing Online Risks

ELSS recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace. We will:

- Regularly review the methods used to identify, assess and minimise online risks.
- Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in the setting is permitted.
- Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.
- Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via our computers or devices.

All members of the community are made aware of our expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community. This is clearly outlined in our acceptable use policies and highlighted through a variety of education and training approaches.

7. Safer Use of Technology

7.1 Classroom Use

ELSS uses a wide range of technology. This includes access to:

- Computers, laptops and other digital devices
- Internet which may include search engines and educational websites
- Email
- Digital cameras, web cams and video cameras

All setting owned devices will be used in accordance with our acceptable use policies and with appropriate safety and security measures in place. Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home. The setting will use age appropriate search tools following an informed risk assessment, to identify which tool best suits the needs of our community. We will ensure that the use of internet-derived materials, by staff and pupils complies with copyright law and acknowledge the source of information. Supervision of pupils will be appropriate to their age and ability.

7.2 Managing Internet Access

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

7.3 Filtering and Monitoring

7.3.1 Decision Making

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

7.3.2 Filtering

The insert internet provider and filter system to ensure that there is adequate filtering of inappropriate content. If pupils discover unsuitable sites, they will be required to:

- Turn off monitor/screen and report the concern immediate to a member of staff.
- The member of staff will report the concern (including the URL of the site if possible) to the DSL (or deputies) and/or technical staff.
- The breach will be recorded and escalated as appropriate.
- Parents/carers will be informed of filtering breaches involving their child.
- Any material believed to be illegal will be reported immediately to the appropriate agencies, such as the Police or CEOP.

7.3.3 Monitoring

We will appropriately monitor internet use on all setting owned or provided internet enabled devices. This is achieved by:

- Use of our monitoring systems for filtering.
- Reports are sent to the Safeguarding team to investigate
- If a concern is identified via monitoring approaches we will inform Safeguarding team will respond in line with the child protection policy.
- All users will be informed that use of our systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

7.4 Managing Personal Data Online

Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations and Data Protection legislation.

7.5 Security and Management of Information Systems

We take appropriate steps to ensure the security of our information systems, including:

- Virus protection being updated regularly.
- Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
- Not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use.
- Not downloading unapproved software to work devices or opening unfamiliar email attachments.
- Regularly checking files held on our network,
- The appropriate use of user logins and passwords to access our network.
- All users are expected to log off or lock their screens/devices if systems are unattended.

7.5.1 Password policy

All members of staff will have their own unique username and private passwords to access our systems; members of staff are responsible for keeping their password private. All pupils are provided with their own unique username and private passwords to access our systems; pupils are responsible for keeping their password private. We require all users to:

- Use strong passwords for access into our system.
- Change their passwords when prompted throughout the year
- Always keep their password private; users must not share it with others or leave it where others can find it.
- Not to login as another user at any time.

7.6 Managing the Safety of our Website

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

7.7 Publishing Images and Videos Online

We will ensure that all images and videos shared online are used in accordance with the associated polices, including (but not limited to) the: acceptable use policies, codes of conduct and staff handbook.

7.8 Managing Email

Access to our email systems will always take place in accordance with data protection legislation and in line with other policies, including confidentiality, acceptable use policies and the code of conduct and scholarly behaviour policy.

- The forwarding of any chain messages/emails is not permitted.
- Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.
- Setting email addresses and other official contact details will not be used for setting up personal social media accounts.
- Members of the community will immediately inform Jennifer Copestake DSL if they receive offensive communication, and this will be recorded in our safeguarding files/records.
- Excessive social email use can interfere with teaching and learning and will be restricted; access to external personal email accounts may be blocked on site.

7.8.1 Staff email

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

7.8.2 Pupil email

Pupils will use provided email accounts for educational purposes. Pupils will read the acceptable use policy and will receive education regarding safe and appropriate email etiquette before access is permitted.

7.9 Live Stream Lessons for Remote Learning

Live stream is a somewhat broad term and, in some cases, can refer to a platform where the teacher and the children are all linked into a video call/conference and see one another. In other cases, it may refer to a live broadcast, where only the teacher, or whoever is providing the content, is visible and the children are viewing the content, without being seen themselves. In the latter example, although not linked into the broadcast with their images, the children may be able to interact through a live chat function. When planning the use of live stream platforms within remote learning our school will:

- Consider whether the technology is available to children/families and make alternative arrangements for provision where necessary.
- Ensure that staff are trained to use the technology.
- Ensure that children's behaviour/interactions are managed in line with the expectations of the school behaviour policy.
- Risk assess the platform being used and consider whether there are functions, such as live chat, pupil's use of video camera, or the recording of the session, which need to be disabled or which require further measures to support their appropriate use.

The above points are relevant to live stream in its broadest sense. What follows next is more relevant, but not exclusively, to the use of platforms allowing two-way video interaction between all users.

- Sessions will be planned and scheduled for during school hours.
- Parents will be contacted to advise that the session is taking place and they and the child should consent to abide to an acceptable use agreement covering issues such as not recording the session, not using the live chat feature, being appropriately dressed etc.
- Only school devices and school contact numbers/emails will be used for communications and running the session.
- Only live streaming platforms approved by SLT will be used.
- Staff will dress professionally and choose a neutral background for their video stream.
- Pupils should be dressed appropriately e.g. clothes they might wear for a non-uniform day, not pyjamas.
- Pupils should live stream from a suitable location within their household, not bedrooms.
- Staff behaviour and language will be entirely in line with the staff code of conduct.
- All other school policies/practices should be followed, notably the safeguarding and child protection policy so should there be any welfare concerns about the child these should be brought to the attention of the DSL without delay. Live Stream from other providers
- When directing pupils to any content from other providers, its suitability and appropriateness will be checked.

- Where that content may be live streamed, the safeguarding aspect of how that content is being delivered will be considered e.g. how children are able to interact, how is content and interactions being monitored/moderated etc?

Using video calls for 1:1 sessions with children

- The school may consider using 1:1 video call sessions to support interventions with children such as mental health support or counselling.
- These sessions will only be provided where they have been risk assessed and approved by SLT.

7.10 Management of Learning Platforms

Leaders and staff will regularly monitor the usage of the Learning Platform (Teams), including message/communication tools and publishing facilities.

- Only current members of staff, pupils and parents will have access to the LP.
- When staff and/or pupils leave the setting, their account will be disabled or transferred to their new establishment.
- Pupils and staff will be advised about acceptable conduct and use when using the LP.
- All users will be mindful of copyright and will only upload appropriate content onto the LP.
- Any concerns about content on the LP will be recorded and dealt with in the following ways:
    - The user will be asked to remove any material deemed to be inappropriate or offensive.
    - If the user does not comply, the material will be removed by the site administrator.
    - Access to the LP for the user may be suspended.
    - The user will need to discuss the issues with a member of leadership before reinstatement.
    - A pupil's parents/carers may be informed.
    - If the content is illegal, we will respond in line with existing child protection procedures.

Pupils may require editorial approval from a member of staff. This may be given to the pupil to fulfil a specific aim and may have a limited time frame. A visitor may be invited onto the LP by a member of the leadership; in this instance, there may be an agreed focus or a limited time slot.

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

We use SchoolPod to track pupils progress and share appropriate information with parents and carers. The Principal is ultimately responsible for the security of any data or images held of children. As such, they will ensure that the use of tracking systems is appropriately risk assessed

prior to use, and that they are used in accordance with data protection legislation, including the General Data Protection Regulations (GDPR) and Data Protection legislation. To safeguard pupil's data:

- Only pupil issued devices will be used for apps that record and store pupils' personal details, attainment or photographs.
- Personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store pupils' personal details, attainment or images.
- Devices will be appropriately encrypted if taken off site, to reduce the risk of a data security breach, in the event of loss or theft.
- All users will be advised regarding safety measures, such as using strong passwords and logging out of systems.
- Parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images.

8. Social Media

8.1 Expectations

The expectations' regarding safe and responsible use of social media applies to all members of East London Science School. The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger.

All members of ELSS are expected to engage in social media in a positive, safe and responsible manner.

All members of ELSS are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others. We will control pupil and staff access to social media whilst using setting provided devices and systems on site.

- The use of social media during setting hours for personal use is not permitted.
- Inappropriate or excessive use of social media during setting hours or whilst using setting devices may result in disciplinary or legal action and/or removal of internet facilities.
- Concerns regarding the online conduct of any member of ELSS community on social media, should be reported to the DSL (or deputy) and will be managed in accordance with our anti-bullying, allegations against staff, behaviour and child protection policies.

8.2 Staff Personal Use of Social Media

The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and

communicated via regular staff training opportunities. Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of our code of conduct.

Reputation

All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the setting. Civil, legal or disciplinary action may be taken if staff are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

All members of staff are advised to safeguard themselves and their privacy when using social media sites. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include (but is not limited to):

- Setting the privacy levels of their personal sites.
- Being aware of location sharing services.
- Opting out of public listings on social networking sites.
- Logging out of accounts after use.
- Keeping passwords safe and confidential.
- Ensuring staff do not represent their personal views as that of the setting.

Members of staff are encouraged not to identify themselves as employees of ELSS on their personal social networking accounts; this is to prevent information on these sites from being linked with the setting, and to safeguard the privacy of staff members. All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance our policies and the wider professional and legal framework.

Information and content that staff members have access to as part of their employment, including photos and personal information about pupils and their family members or colleagues will not be shared or discussed on social media sites.

Members of staff will notify the Senior Leadership Team immediately if they consider that any content shared on social media sites conflicts with their role.

Communicating with pupils and parents and carers

All members of staff are advised not to communicate with or add as 'friends' any current or past pupils or their family members via any personal social media sites, applications or profiles.

- Any pre-existing relationships or exceptions that may compromise this, will be discussed with DSL (or deputies) and/or the Principal.
- If ongoing contact with pupils is required once they have left the setting, members of staff will be expected to use existing alumni networks or use official setting provided communication tools.

Staff will not use personal social media accounts to contact pupils or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the

Principal. Any communication from pupils and parents received on personal social media accounts will be reported to the DSL (or deputies).

8.3 Pupils Personal Use of Social Media

Safe and appropriate use of social media will be taught to pupils as part of an embedded and progressive education approach, via age appropriate sites and resources. Any concerns regarding pupils use of social media will be dealt with in accordance with existing policies, including anti-bullying and Scholarly Behaviour.

- Concerns will be shared with parents/carers as appropriate, particularly when concerning underage use of social media sites, games or tools.

Pupils will be advised:

- To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location.
- To only approve and invite known friends on social media sites and to deny access to others by making profiles private.
- Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.
- To use safe passwords.
- To use social media sites which are appropriate for their age and abilities.
- How to block and report unwanted communications.
- How to report concerns both within the setting and externally.

8.4 Official Use of Social Media

ELSS official social media channels are a twitter account, a facebook page and an Instagram account.

The official use of social media sites only takes place with clear educational or community engagement objectives, with specific intended outcomes. Official social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only. Staff use setting provided email addresses to register for and manage any official social media channels. Official social media sites are suitably protected and linked to our website. Public communications on behalf of the setting will, where appropriate and possible, be read and agreed by at least one other colleague.

Official social media use will be conducted in line with existing policies, including: antibullying, scholarly behvaiour, data protection, safeguarding and child protection. All communication on official social media platforms will be clear, transparent and open to scrutiny.

Parents/carers and pupils will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community. Only social media tools which have been risk assessed and approved as suitable for educational purposes will be used

Staff expectations

- Members of staff who follow and/or like our official social media channels will be advised to use dedicated professionals accounts, where possible, to avoid blurring professional boundaries.
- If members of staff are participating in online social media activity as part of their capacity as an employee of the setting, they will:
    - Read this policy and acceptable use policy.
    - Always be professional and aware they are an ambassador for the setting.
    - Disclose their official role but make it clear that they do not necessarily speak on behalf of the setting.
    - Always be responsible, credible, fair and honest, and consider how the information being published could be perceived or shared.
    - Always act within the legal frameworks they would adhere to within the workplace, including: libel, defamation, confidentiality, copyright, data protection and equalities laws.
    - Ensure that they have appropriate consent before sharing images on the official social media channel.
    - Not disclose information, make commitments or engage in activities on behalf of the setting, unless they are authorised to do so.
    - Not engage with any direct or private messaging with current, or past, pupils, parents and carers.
    - Inform their line manager, the DSL (or deputies) and/or the Principal of any concerns, such as criticism, inappropriate content or contact from pupils.

9. Use of Personal Devices and Mobile Phones

ELSS recognises that personal communication through mobile technologies is an accepted part of everyday life for pupils, staff and parents/carers, but technologies need to be used safely and appropriately within the setting.

9.1 Expectations

All use of personal devices (including but not limited to; tablets, games consoles and 'smart' watches) and mobile phones will take place in accordance with the law and other appropriate policies, such as anti-bullying, behaviour and child protection.

Electronic devices of any kind that are brought onto site are the responsibility of the user.

- Pupils are informed that if their electronic devices are seen or heard in the school setting they will be confiscated. Further clarification can be found in our Scholarly Behaviour Policy.
- All members of ELSS community are advised to take steps to protect their mobile phones or devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises.
- All members of ELSS community are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared.
- Mobile phones and personal devices are not permitted to be used in specific areas within the site such as changing rooms and pupil toilets.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with as part of our behaviour policy.
- All members of ELSS are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or would otherwise contravene our behaviour or child protection policies.

9.2 Staff Use of Personal Devices and Mobile Phones

Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as, relevant policy and procedures, such as: Safeguarding and child protection, data security and acceptable use. Staff will be advised to:

- Keep mobile phones and personal devices in a safe and secure place during lesson time.
- Keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times.
- Ensure that Bluetooth or other forms of communication (such as 'airdrop') are hidden or disabled during lesson times.
- Ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations.

Members of staff are advised against using their own personal phones or devices for contacting pupils or parents and carers. Permission should be sought with exceptional circumstances and the staff number hidden.

- Any pre-existing relationships, which could undermine this, will be discussed with the DSL (or deputies) and/or Principal.

If a member of staff breaches our policy, action will be taken in line with our code of conduct and allegations policy. If a member of staff is thought to have illegal content saved or stored on a

mobile phone or personal device or have committed a criminal offence, the police will be contacted.

9.**3 Pupils Use of Personal Devices and Mobile Phones**

Pupils will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences. ELSS expects pupils' personal devices and mobile phones to be switched off and out of sight during the school day. If a pupil needs to contact his/her parents or carers they should contact their Head of Year or Reception who will contact the parent/carer.

Parents are advised to contact their child via the setting office; exceptions may be permitted on a case-by-case basis, as approved by the Principal.

Mobile phones or personal devices will not be used by pupils during lessons or formal educational time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.

- The use of personal mobile phones or devices for a specific education purpose does not mean that blanket use is permitted.
- If members of staff have an educational reason to allow pupils to use their mobile phones or personal devices as part of an educational activity, it will only take place when approved by the Senior Leadership Team.

Mobile phones and personal devices must not be taken into examinations.

- Pupils found in possession of a mobile phone or personal device during an exam will be reported to the appropriate examining body. This may result in the withdrawal from either that examination or all examinations.

If a pupil breaches the policy, the phone or device will be confiscated and will be held in a secure place.

- Staff may confiscate a pupil's mobile phone or device if they believe it is being used to contravene our behaviour or bullying policy or could contain youth produced sexual imagery (sexting).
- Searches of mobile phone or personal devices will only be carried out in accordance with the following guidance. www.gov.uk/government/publications/searching-screening-andconfiscation
- Pupils mobile phones or devices may be searched by a member of the leadership team, with the consent of the pupil or a parent/ carer. Content may be deleted or requested to be deleted, if it contravenes our policies. www.gov.uk/government/publications/searching-screening-and-confiscation
- Mobile phones and devices that have been confiscated will be either released to the pupil or the parents or carers depending on a case by case situation.

- If there is suspicion that material on a pupil's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.

9.4 Visitors' Use of Personal Devices and Mobile Phones

Parents/carers and visitors (including volunteers and contractors) must use their mobile phones and personal devices in accordance with our acceptable use policy and other associated policies, such as: anti-bullying, scholarly behaviour, safeguarding and child protection.

We will ensure appropriate signage and information is displayed and provided to inform parents, carers and visitors of expectations of use.

Members of staff are expected to challenge visitors if they have concerns and will always inform the DSL (or deputies) or Principal of any breaches our policy.

9.5 Officially provided mobile phones and devices

School mobile phones and devices will be suitably protected via a passcode/password/pin and must only be accessed or used by members of staff. School mobile phones and devices will always be used in accordance with the acceptable use policy and associated policies, such as: anti-bullying, scholarly behaviour, safeguarding and child protection.

10. Responding to Online Safety Incidents and Concerns

All members of the community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting), cyberbullying and illegal content.

All members of the community must respect confidentiality and the need to follow the official procedures for reporting concerns. Pupils, parents and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.

We require staff, parents, carers and pupils to work in partnership to resolve online safety issues. After any investigations are completed, we will debrief, identify lessons learnt and implement any policy or curriculum changes as required. Safeguarding concerns and incidents should be reported to the DSL and Safeguarding team or the Local Authority MASH.

Where there is suspicion that illegal activity has taken place, we will contact the Police via our safer schools officer, or using 101, or 999 if there is immediate danger or risk of harm.

If an incident or concern needs to be passed beyond our community (for example if other local settings are involved or the public may be at risk), the DSL or Principal will speak with Police and to ensure that potential investigations are not compromised.

10.1 Concerns about Pupils Welfare

The DSL (or deputies) will be informed of any online safety incidents involving safeguarding or child protection concerns. The DSL (or deputies) will record these issues in line with our child protection policy.

The DSL (or deputies) will ensure that online safety concerns are escalated and reported to relevant agencies. We will inform parents and carers of online safety incidents or concerns involving their child, as and when required.

10.2 Staff Misuse

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

11. Procedures for Responding to Specific Online Incidents or Concerns

11.1 Online Sexual Violence and Sexual Harassment between Children

Our school has accessed and understood "Sexual violence and sexual harassment between children in schools and colleges" (2021) guidance and part 5 of 'Keeping children safe in education' 2021. ELSS recognises that sexual violence and sexual harassment between children can take place online. Examples may include; non-consensual sharing of sexual images and videos, sexualised online bullying, online coercion and threats, unwanted sexual comments and messages on social media, and online sexual exploitation.

Full details of how we will respond to concerns relating to sexual violence and sexual harassment between children can be found within our Safeguarding and Child Protection and anti-bullying policy.

ELSS recognises that internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities.

ELSS also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.

ELSS will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment between children through relevant explanations and learning method though our personal development curriculum.

We will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between children.

We will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.

If made aware of online sexual violence and sexual harassment, we will:

- Immediately notify the DSL (or deputy) and act in accordance with our safeguarding and child protection and anti-bullying policies.
- If content is contained on pupils electronic devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
- Provide the necessary safeguards and support for all pupils involved, such as offering specific advice on blocking, reporting and removing online content, as well as providing appropriate counselling/pastoral support.
- Implement appropriate sanctions in accordance with our scholarly behaviour policy.
- Inform parents and carers, if appropriate, about the incident and how it is being managed.
- If appropriate, make a referral to partner agencies, such as Children's Social Care and/or the Police.
- If the concern involves children and young people at a different educational setting, work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community.
- If a criminal offence has been committed, the DSL (or deputy) will discuss this with the Police first to ensure that investigations are not compromised.
- Review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.

11.2 Youth Produced Sexual Imagery ("Sexting")

ELSS recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy). We will follow the advice as set out in the non-statutory UKCCIS guidance: 'Sexting in schools and colleges: responding to incidents and safeguarding young people'. ELSS ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of 'sexting' by implementing preventative approaches.

We will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery. We will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on/off site or using setting provided or personal equipment.

We will not:

- View any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so.
- If it is deemed necessary, the image will only be viewed by the DSL (or deputy DSL) and their justification for viewing the image will be clearly documented.
- Send, share, save or make copies of content suspected to be an indecent image of a child (i.e. youth produced sexual imagery) and will not allow or request pupils to do so.

If made aware of an incident involving the creation or distribution of youth produced sexual imagery, we will:

- Act in accordance with our child protection policies and the relevant Local Authority Safeguarding Child Board's procedures.
- Ensure the DSL (or deputy) responds in line with the 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
- Store the device securely.
- If an indecent image has been taken or shared on our network or devices, we will act to block access to all users and isolate the image.
- Carry out a risk assessment which considers any vulnerability of pupils involved; including carrying out relevant checks with other agencies.
- Inform parents and carers, if appropriate, about the incident and how it is being managed.
- Make a referral to Children's Social Care and/or the Police, as appropriate.
- Provide the necessary safeguards and support for pupils, such as offering counselling or pastoral support.
- Implement appropriate sanctions in accordance with our scholarly behaviour policy but taking care not to further traumatise victims where possible.
- Consider the deletion of images in accordance with the UKCCIS: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
- Images will only be deleted once the DSL has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation.
- Review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.

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

ELSS will ensure that all members of the community are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.

ELSS recognises online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL (or deputy). We will implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability appropriate education for pupils, staff and parents/carers. We will ensure that all members of the community are aware of the support available regarding online child sexual abuse and exploitation (including criminal exploitation), both locally and nationally.

If made aware of incident involving online child sexual abuse and exploitation (including criminal exploitation), we will:

- Act in accordance with our child protection policies and the relevant Local Authority Safeguarding Child Board's procedures.
- If appropriate, store any devices involved securely.

- Make a referral to Children's Social Care (if required/ appropriate) and immediately inform the police via 101 (or 999 if a child is at immediate risk)
- Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).
- Inform parents/carers about the incident and how it is being managed.
- Provide the necessary safeguards and support for pupils, such as, offering counselling or pastoral support.
- Review the handling of any incidents to ensure that best practice is implemented; leadership team will review and update any management procedures, where necessary.

We will respond to concerns regarding online child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on our premises or using setting provided or personal equipment. Where possible, pupils will be involved in decision making and if appropriate, will be empowered to report concerns such as via the Click CEOP report: www.ceop.police.uk/safety-centre/

If we are unclear whether a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through Police. If pupils at other setting are believed to have been targeted, the DSL (or deputy) will seek support from the Police first to ensure that potential investigations are not compromised.

11.4 Indecent Images of Children (IIOC)

ELSS will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC). We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site. We will seek to prevent accidental access to IIOC by using an internet Service provider (ISP) which subscribes to the accredited block list and by implementing appropriate filtering, firewalls and anti-spam software.

If we are unclear if a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Police.

If made aware of IIOC, we will:

- Act in accordance with our safeguarding and child protection policy and the relevant local authority Safeguarding Child Boards procedures.
- Store any devices involved securely.
- Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), police or the LADO.

If made aware that a member of staff or a pupil has been inadvertently exposed to indecent images of children, we will:

- Ensure that the DSL (or deputy DSL) is informed.

- Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk
- Ensure that any copies that exist of the image, for example in emails, are deleted.
- Report concerns, as appropriate to parents and carers.

If made aware that indecent images of children have been found on the setting provided devices, we will:

- Ensure that the DSL (or deputy DSL) is informed.
- Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk
- Ensure that any copies that exist of the image, for example in emails, are deleted.
- Inform the police via 101 (999 if there is an immediate risk of harm) and children's social services (as appropriate).
- Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
- Report concerns, as appropriate to parents and carers.

If made aware that a member of staff is in possession of indecent images of children on setting provided devices, we will:

- Ensure that the Principal is informed in line with our managing allegations against staff policy.
- Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with our managing allegations against staff policy.
- Quarantine any devices until police advice has been sought.

11.5 Cyberbullying

Cyberbullying, along with all other forms of bullying, will not be tolerated at ELSS. Full details of how we will respond to cyberbullying are set out in our anti-bullying policy which is published on our website.

11.6 Online Hate

Online hate content, directed towards or posted by, specific members of the community will not be tolerated at ELSS and will be responded to in line with existing policies, including anti-bullying and scholarly behaviour.

All members of the community will be advised to report online hate in accordance with relevant policies and procedures. The Police will be contacted if a criminal offence is suspected. If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL (or deputy DSL) will obtain advice through the safer schools officer or Police.

11.7 Online Radicalisation and Extremism

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

If we are concerned that a child or parent/carer may be at risk of radicalisation online, the DSL (or deputy DSL) will be informed immediately, and action will be taken in line with our child protection policy. If we are concerned that member of staff may be at risk of radicalisation online, the Principal will be informed immediately, and action will be taken in line with the child protection and allegations policies.

12. Useful Links for Educational Settings

Newham Support and Guidance:

If you are concerned about a child in Newham contact Newham Child Protection (MASH):

Office Hours (Mon-Thu 9am-5.15pm and Fri 9am-5pm) - 0203 373 4600

Out of Office Hours - 0208 430 2000

Newham Prevent Team - 020 3373 0440

Newham Safeguarding Children's Partnership https://www.newhamscp.org.uk/stay-safe-online/

Tower Hamlets Support and Guidance:

If you are concerned about a child in Tower Hamlets contact Tower Hamlets Child Protection (MASH):

Office Hours (Mon-Thu 9am-5.00pm) - 0207 364 5006

Out of Office Hours - 0207 364 4079

Tower Hamlets Prevent as part of MASH – 0207 364 3009

Newham Safeguarding Children's Partnership http://www.childrenandfamiliestrust.co.uk/the-lscb/

Police Support and Guidance

Metropolitan Police: https://www.met.police.uk/

For non-urgent Police contact 101

If you think the child is in immediate danger, you should call the police on 999.

National Links and Resources for Educational Settings

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

Childnet: www.childnet.com

Internet Matters: www.internetmatters.org

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

Lucy Faithfull Foundation: www.lucyfaithfull.org

NSPCC: www.nspcc.org.uk/onlinesafety

ChildLine: www.childline.org.uk

Net Aware: www.net-aware.org.uk

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

UK Safer Internet Centre: www.saferinternet.org.uk

Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline

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

National Links and Resources for Parents/Carers

Action Fraud: www.actionfraud.police.uk

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

Childnet: www.childnet.com

Get Safe Online: www.getsafeonline.org

Internet Matters: www.internetmatters.org

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

Lucy Faithfull Foundation: www.lucyfaithfull.org

NSPCC: www.nspcc.org.uk/onlinesafety

ChildLine: www.childline.org.uk

Net Aware: www.net-aware.org.uk

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

UK Safer Internet Centre: www.saferinternet.org.uk

There is a wealth of information available to support schools and parents/carers to keep children safe online. See Keeping Children Safe in Education 2021 (Annex D) for more resources.

APPENDIX – A

Acceptable Use of ICT for Staff, Approved Guests & Volunteers Policy

ELSS Staff ICT Acceptable Use Policy

This Acceptable Use Policy is intended to ensure:

- that staff, volunteers and approved guests, such as ITT, will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of ICT in their everyday work.

ELSS provides a range of ICT resources which are available to all staff. In order to ensure the safety of both staff and pupils, it is important that all staff follow the guidelines detailed below.

Terms of Acceptable Use:

Application of policy: This policy applies to all staff of the school and volunteers, including approved guests regardless of their use of ICT systems

School Email

Every member of staff is provided with a school email address. The email system can be accessed from both the school computers, and via the internet from any device.

The sending of emails is subject to the following rules:

- I will always communicate in a professional manner.
- Language must not include swear words, or be offensive or abusive.
- Emails or attachments of a pornographic, illegal, violent, sexist or racist nature, terrorist and extremist material are not permitted.
- Sending of attachments which contain copyright material to which the school does not have distribution rights is not permitted.

Limited personal use of the email system is permitted, provided that it complies with the guidelines set out in section 4 of this policy, and that any content complies with the rules above. Staff should keep levels of personal email to a minimum.

All email within the school is monitored, and email accounts can be checked in order to ensure compliance with the above rules.

All staff should be aware that email is not a secure communications medium, and therefore careful consideration should be given before the transmission of confidential files or staff / pupil data.

Staff volunteers and approved guests are not permitted to send via email any information which is covered by the Data Protection Act, without prior written authorisation from the schools data protection officer.

Internet Access

The school provides internet access for all staff and pupils in order to allow access to the wide range of content available. The schools' internet connection is filtered, meaning that a large amount of inappropriate material is not accessible. However, on occasion it may be possible to view a website which is inappropriate for use in a school. In which case the website must be reported in writing (e-mail) to the IT Manager.

It is not permitted to attempt to access, on any device, pornographic, illegal, sexist, violent, racist, extreme, terrorist or other inappropriate material in school.

Members of the IT Team have access to an unfiltered internet connection. Access is still only permitted to appropriate websites, unless directly instructed by the Principal.

The use of online real-time chat rooms is banned, unless specific permission is sought from the Head Teacher.

No member of staff may download any software from the internet for installation onto a school computer system without prior written authorisation from the Principal.

Personal use of Equipment

The ICT provisions provided by the school are for work relating to the School. However, the school acknowledges that, on occasion it may be necessary to use the ICT equipment for personal use. This is permitted provided that:

- Any activities carried out on them complies with the other terms of this policy.
- No personal applications are loaded onto any computers.
- Any activity completed on school equipment does not result in personal gain for the member of staff involved.
- The removal of ICT equipment from the school site for personal use is only permitted with the consent of the Head teacher or Business Manager. The exception to this is any equipment assigned to, and signed for by individual members of staff.

Individuals are responsible for the cost of any personal phone calls. All calls are logged and may be recorded.

All staff members are responsible for reporting their own personal use of a school computer, and any associated tax costs this has.

No technical support is provided by the school for problems arising as a result of personal work on the equipment.

Digital Photography

The school encourages the use of digital cameras and video equipment; however, staff should be aware of the following guidelines:

Photos should only be named with the pupils' name if permission has been given from the parents via the entry form.

The updated list can be accessed via SchoolPod.

The use of digital photography in school is permitted. However, images of pupils must be downloaded to the school network and removed from the camera before it leaves the school site. All photos should be downloaded to the school network

Security

Each member of staff is allocated a username and password. Staff are responsible for ensuring their password remains a secret and their account is secure. Staff are not permitted to write their password down.

Under no circumstances should a pupil be allowed to use a staff computer account, unless being directly supervised by the account owner for the purposes of curriculum use. When any pc is left unattended, it must either be logged off or locked. No member of staff may use a computer which is found logged on as someone else, it must be immediately logged off.

Passwords are recommended to be changed regularly, this will be prompted on the device. Staff will only access areas of the schools' computer systems to which they have been authorised access.

File Storage

Each member of staff has their own personal area on the network, as well as access to shared network drives. Any school related work should be stored on one of these network drives.

Staff must not access, remove or otherwise alter any other user's file, without their express permission.

All staff should be aware that all files must be stored on a network shared area in order that they will be backed up. Files lost from a USB key are not recoverable. Staff are responsible for ensuring they have rights for the storage of any file in their area, for example copyright music files.

Any files stored on removable media must be stored in accordance with the following: No school data is to be stored on a home computer, or un-encrypted storage device. No confidential, or School data which is subject to the Data Protection Act should be transferred off site using unsecured email. Any pupil data will be kept private and confidential, except when it is deemed necessary by school policy or law to disclose such information to the appropriate authority.

Mobile Phones

All phone contact with parents regarding school issues should be through the schools' phones where possible. If a personal phone has to be used then care must be taken by the member of staff to ensure their number is withheld.

Social networking

Please refer to the Schools Online Safety Policy.