St. Joseph's R.C. Primary School

Online Safety Policy

Policy Completed By: Mrs Byrne

Date for Review: Spring 2021

<u>St. Joseph's School Online Safety Policy</u>

<u>Our School Mission Statement</u>

At St. Joseph's School, we aim to grow and learn together within a loving and caring environment which reflects the Gospel values. We encourage all our children to reach their full potential in all aspects of their education.

1.   Policy Aims

- This online safety policy has been written by St. Joseph's Headteacher with contributions from staff, learners and parents/carers, building on the Kent County Council online safety policy template, with specialist advice and input as required.
- It takes into account the DfE statutory guidance '<u>Keeping Children Safe in Education</u>' 2019, <u>Early Years and Foundation Stage</u> 2017, '<u>Working Together to Safeguard Children</u>' 2018 and the <u>Schools Safeguarding Forum</u> procedures.

- The purpose of St. Joseph's Online Safety Policy is to:
  - Safeguard and protect all members of St. Joseph's 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.

2.   Policy Scope

- St. Joseph's believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all learners and staff are protected from potential harm online.
- St. Joseph's identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life.
- St. Joseph's believes that learners should be empowered to build resilience and to develop strategies to manage and respond to risk online.
- This policy applies to all staff including the governing body, leadership team, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the setting (collectively referred to as "staff" in this policy) as well as learners, parents and carers.
- This policy applies to all access to the internet and use of technology, including personal devices.

  2.1.   Links with other policies and practices:
  - Anti-bullying Policy
  - Acceptable Use Policies (AUP) and the Code of Conduct
  - Behaviour Policy

- o Safeguarding (Child Protection) Policy
- o Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE) and Relationships and Health Education (RHE)
- o Data Protection policy

3. Monitoring and Review

- Technology in this area evolves and changes rapidly. St. Joseph's will review this policy at least annually.
    - o 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 *Headteacher and PSHE coordinator* will be informed of online safety concerns, as appropriate.
- The named governor for safeguarding *(Mr Metzgen)* 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) *(Mrs Byrne, Headteacher)* has lead responsibility for online safety.
- St. Joseph's recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

4.1. The Senior Management Team (SMT) 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 acceptable use policy, which covers acceptable use of technology.
- Ensure that suitable and appropriate filtering and monitoring systems are in place and work with technical staff to monitor the safety and security of our systems and networks.
- Ensure that online safety is embedded within a progressive curriculum, which enables all learners 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 and up to date knowledge required to keep learners safe online.
- Access regular and appropriate training and support to ensure they recognise the additional risks that learners with SEN and disabilities (SEND) face online.
- 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.
- Work with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input.
- Meet regularly (*once a term*) with the governor with a lead responsibility for safeguarding and 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 acceptable use policies.
- Take responsibility for the security of setting systems and the data they use or have access to.
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.
- Embed online safety education in curriculum delivery, wherever possible.
- Have an awareness of a range of online safety issues and how they may be experienced by the children in their care.
- Identify online safety concerns and take appropriate action by following the settings safeguarding policies and procedures.

- Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.

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

- Provide technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Implement appropriate security measures as directed by the leadership team to ensure that the settings IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensure that our filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- Ensure that our monitoring systems are applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team
- Ensure appropriate access and technical support is given to the DSL (and/or deputy) to our filtering and monitoring systems, to enable them to take appropriate safeguarding action if/when required.

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

- Engage in age appropriate online safety education opportunities.
- Contribute to the development of online safety policies.
- Read and adhere to the acceptable use policies.
- Respect the feelings and rights of others both on and offline.
- Take responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues.

4.6.   It is the responsibility of parents and carers to:

- Read the acceptable use policies and encourage their children to adhere to them.
- Support our online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home.
- Role model safe and appropriate use of technology and social media.
- Abide by the home-school agreement and acceptable use policies.
- Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the setting, or other appropriate agencies, if they or their child encounter risk or concerns online.
- 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 & Engagement with learners

- The setting will establish and embed a progressive online safety curriculum to raise awareness and promote safe and responsible internet use amongst learners by:
    - o Ensuring education regarding safe and responsible use precedes internet access.
    - o Including online safety in Personal, Social, Health and Economic (PSHE), Relationships and Sex Education (RSE) and computing programmes of study.
    - o Reinforcing online safety messages whenever technology or the internet is in use.
    - o Educating learners in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
    - o Teaching learners to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

- The setting will support learners to read and understand the acceptable use policies in a way which suits their age and ability by:
    - o Displaying acceptable use posters in all rooms with internet access.
    - o Informing learners that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
    - o Rewarding positive use of technology.
    - o Implementing appropriate peer education approaches.
    - o Providing online safety education and training as part of the transition programme across the key stages and when moving between establishments.
    - o Seeking learner voice when writing and developing online safety policies and practices, including curriculum development and implementation.
    - o Using support, such as external visitors, where appropriate, to complement and support our internal online safety education approaches.

5.2.   Vulnerable Learners

- St. Joseph's recognises that some learners 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.
- St. Joseph's will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable learners.

- When implementing an appropriate online safety policy and curriculum St. Joseph's will seek input from specialist staff as appropriate, including the SENCO *(Mrs Schönknecht)*, Child in Care Designated Teacher. (*Mrs Byrne*)

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.
  - As part of existing safeguarding and child protection training/updates and within specific online safety sessions during INSET or staff meeting.
  - This will cover the potential risks posed to learners (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 learners.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting learners, colleagues or other members of the community.

5.4. Awareness and engagement with parents and carers

- St. Joseph's 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, transition events, etc.
  - Drawing their attention to the online safety policy and expectations in newsletters, letters, our prospectus and on our website.
  - Requesting that they read online safety information as part of joining our community, for example, within our home school agreement.
  - Requiring them to read our acceptable use policies and discuss the implications with their children.

6.   Reducing Online Risks

- St. Joseph's recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace.
- We will:
  - o Regularly review the methods used to identify, assess and minimise online risks.
  - o Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in the setting is permitted.
  - o Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.
  - o 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

- St. Joseph's uses a wide range of technology. This includes access to:
  - o Computers, laptops and other digital devices
  - o Internet which may include search engines and educational websites
  - o Learning platform/intranet
  - o Email
  - o Games-based technologies
  - o Digital 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 learners complies with copyright law and acknowledge the source of information.
- Supervision of learners will be appropriate to their age and ability.
  - o **Early Years Foundation Stage and Key Stage 1**
    - ▪ Access to the internet will be by adult demonstration, with occasional directly supervised access to specific and approved online materials,

which supports the learning outcomes planned for the learner's age and ability.

- o **Key Stage 2**
    - Learners will use age-appropriate search engines and online tools.
    - Learners will be directed by the teacher to online materials and resources which support the learning outcomes planned for the learner's age and ability.

7.2 Filtering and Monitoring

7.2.1 Decision Making

- St. Joseph's SMT have ensured that our setting has age and ability appropriate filtering and monitoring in place, to limit learner's exposure to online risks.
- The SMT are aware of the need to prevent "over blocking", as that may unreasonably restrict what can be taught, with regards to online activities and safeguarding.
- Our decision regarding filtering and monitoring has been informed by a risk assessment, considering our specific needs and circumstances.
- Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from the SMT.
- The SMT 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 learners; effective classroom management and regular education about safe and responsible use is essential.

7.2.2 Filtering

- Education broadband connectivity is provided through BT.
- We use London Grid for Learning (*LGFL)* which blocks sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature.
- The filtering system blocks all sites on the [Internet Watch Foundation](#) (IWF) list.
- We work with LGFL to ensure that our filtering policy is continually reviewed.
- If learners discover unsuitable sites, they will be required to:
    - o Turn off monitor/screen and report the concern immediate to a member of staff.
    - o The member of staff will report the concern (including the URL of the site if possible) to the DSL (or deputy) and/or technical staff.
    - o The breach will be recorded and escalated as appropriate.
    - o Parents/carers will be informed of filtering breaches involving their child.
- Any material believed to be illegal will be reported immediately to the appropriate agencies, such as the IWF, Police or CEOP.

7.3 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.
  o Full information can be found in our Data protection policy.

7.4 Security and Management of Information Systems

- We take appropriate steps to ensure the security of our information systems, including:
  o Virus protection being updated regularly.
  o 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.
  o Not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use.
  o Not downloading unapproved software to work devices or opening unfamiliar email attachments.
  o Regularly checking files held on our network.
  o The appropriate use of user logins and passwords to access our network.
    ▪ Specific user logins and passwords will be enforced for all *but the youngest users.* (Early Years and Foundation Stage children)
  o All users are expected to log off or lock their screens/devices if systems are unattended.

7.4.1 Password

- 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.
- From year 1, all learners are provided with their own unique username and private passwords to access our systems; learners are responsible for keeping their password private.
- We require all users to:
  o Use strong passwords for access to our system.
  o Always keep their password private; users must not share it with others or leave it where others can find it.
  o Not to login as another user at any time.

7.5 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; privacy policies and copyright.

- Staff or learners' 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.

7.6 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.
  - o The forwarding of any chain messages/emails is not permitted.
  - o Spam or junk mail will be blocked and reported to the email provider.
  - o Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.
  - o 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 *Mrs Byrne* 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 will be discouraged during the school day.

7.6.1   Staff email

- The use of personal email addresses by staff for any official setting business is not permitted.
  - o 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 or other professionals.

7.6.2   Learner email

- Learners will use email accounts provided for educational purposes.
- Learners will receive education regarding safe and appropriate email etiquette before access is permitted.

8. Social Media

8.1 Expectations

- The expectations regarding safe and responsible use of social media applies to all members of St. Joseph's community.
- The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger.
- All members of St. Joseph's community are expected to engage in social media in a positive, safe and responsible manner.
  - All members of St. Joseph's community 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 learner 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 removal of internet facilities.
- Concerns regarding the online conduct of any member of St. Joseph's community on social media, should be reported to the DSL 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 and as part of our Acceptable Use policy.

8.2.1 Reputation
- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the 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 deemed 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 St. Joseph's 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 with our policies and the wider professional and legal framework.
- Information and content that staff members have access to as part of their employment, including photos and personal information about learners and their family members or colleagues will not be shared or discussed on social media sites.
- Members of staff will notify the Leadership Team immediately if they consider that any content shared on social media sites conflicts with their role.

8.2.2 Communicating with learners and parents and carers
- All members of staff are advised not to communicate with or add as 'friends' any current or past learners 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 deputy).
- Staff will not use personal social media accounts to contact learners or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the headteacher.
- Any communication from learners and parents received on personal social media accounts will be reported to the DSL (or deputy).

8.3 Learners Personal Use of Social Media

- Safe and appropriate use of social media will be taught to learners as part of an embedded and progressive education approach, via age appropriate sites and resources.
- We are aware that many popular social media sites state that they are not for children under the age of 13, therefore we will not create accounts specifically for learners under this age.
- Any concerns regarding learners use of social media will be dealt with in accordance with existing policies, including anti-bullying and behaviour.
    - Concerns will be shared with parents/carers as appropriate, particularly when concerning underage use of social media sites, games or tools.
- Learners 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.

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

9. Use of Personal Devices and Mobile Phones

- St. Joseph's recognises that personal communication through mobile technologies is an accepted part of everyday life for learners, 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.
    - o All members of St. Joseph's 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.
    - o All members of St. Joseph's 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, toilets and swimming pools. The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with as part of our behaviour policy.
- All members of St. Joseph's community are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or would otherwise contravene our behaviour or child protection policies.

9.2 Staff Use of Personal Devices and Mobile Phones

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

- o Keep mobile phones and personal devices in a safe and secure place during lesson time.
- o Keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times.
- o Ensure that Bluetooth or other forms of communication (such as 'airdrop') are hidden or disabled during lesson times.
- o Not use personal devices during teaching periods, unless permission has been given by the SMT, such as in emergency circumstances.
- o 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 not permitted to use their own personal phones or devices for contacting learners or parents and carers.
  - o Any pre-existing relationships, which could undermine this, will be discussed with the DSL (or deputy).
- Staff will not use personal devices:
  - o To take photos or videos of learners and will only use work-provided equipment for this purpose.
  - o Directly with learners and will only use work-provided equipment during lessons/educational activities.
- If a member of staff breaches our policy, action will be taken in line with our code of conduct/staff behaviour and allegations policy
  - o 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 Learners Use of Personal Devices and Mobile Phones

- Learners will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.
- St. Joseph's expects learners' personal devices and mobile phones to be checked in and checked out at pupil reception at the start and end of the school day.
  - o If a parent or carer need to be contacted this will be via a member of admin.
  - o Parents are advised to contact their child via the setting office.
- If a learner breaches the policy, the phone or device will be confiscated and will be held in a secure place.
  - o Staff may confiscate a learner'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).
  - o Learners' mobile phones or devices may be searched by a member of the leadership team, with the consent of the learner or a parent/ carer. Content may be deleted or requested to be deleted, if it contravenes our policies.
  - o Mobile phones and devices that have been confiscated will be released to parents or carers at the end of the day.

- o If there is suspicion that material on a learner'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) should ensure that mobile phones are only permitted within specific areas so they do not disrupt learning.
- Visitors (including volunteers and contractors) who are on site for a regular or extended period will use their mobile phones and personal devices in accordance with our acceptable use policy and other associated policies, such as: anti-bullying, behaviour, child protection and image use.
- Members of staff are expected to challenge visitors if they have concerns and will always inform the DSL (or deputy) of any breaches of our policy.

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.
  - o Learners, parents and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.
- We require staff, parents, carers and learners to work in partnership to resolve online safety issues.
- After any investigations are completed, we will debrief, identify lessons learnt and implement any policy or curriculum changes as required.
- If we are unsure how to proceed with an incident or concern, the DSL (or deputy) will seek advice from the Education Safeguarding Service.
- Where there is suspicion that illegal activity has taken place, we will contact the Education Safeguarding Service or Police using 101, or 999 if there is immediate danger or risk of harm.
- If an incident or concern needs to be passed beyond our community (for example if other local settings are involved or the public may be at risk), the DSL (or deputy) will speak with Police and/or Education Safeguarding Service first to ensure that potential investigations are not compromised.

10.1 Concerns about Learners Welfare

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

- The DSL (or deputy) will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Kent Safeguarding Children Board thresholds and procedures.
- 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 Mrs Byrne, in accordance with the allegations policy.
- Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- Appropriate action will be taken in accordance with our staff behaviour policy/code of conduct.

Appendix 1: Internet use – possible teaching and learning activities

Activities	Key e-safety issues	Relevant websites
Creating web directories to provide easy access to suitable websites	Pupils should be supervised. Pupils should be directed to specific, approved on-line materials	Web directories e.g. keep bookmarks
Using search engines to access information from a range of websites	Filtering must be active and checked frequently Pupils should be supervised Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with	Web guests e.g. Google Chrome / Internet Explorer CBBC search
Exchanging information with other pupils and asking questions of experts via e-mail or blogs	Pupils should only use approved e-mail or blogs Pupils should never give out personal information Consider using systems that provide on-line moderation	e-mail
Publishing pupils' work on school and other websites	Pupil and parental consent should be sought prior to publication Pupils' full names and other personal information should be omitted Pupils work should only be published on 'moderated sites' and by the school administrator	
Communicating ideas within chat rooms or online forums	Chat rooms are not permitted. Access to other social networking sites should have restricted access. Pupils should never give out personal information. Pupils should be supervised when using secure school e-mail accounts.	

Appendix 2: Useful resources for teachers

BBC stay Safe
www.bbb.co.uk/cbbc/help/safesurfing/

Becta
http://schools.becta.org.uk/index.php?section=i

Chat Danger
www.chatdanger.com/

Child Exploitation and Online Protection Centre
www.ceop.gov.uk/

Childnet
www.childnet-int.org/

Cyber Café
http://thinkuknow.co.uk/8_10/cybercafe/cafe/base.aspx

Digizen
www.digizen.org/

Kent e-safety Policy and Guidance, Posters etc.
www.clusterweb.org.uk/kcn/e-safetyhome.cfm

Kidsmart
www.kidsmart.org.uk/

Think U Know
www.thinkuknow.co.uk/

Safer Children in the Digital World
www.dfes.gov.uk/byronreview/

Appendix 3: Useful resources for parents

Care for the family
www.careforthefamily.org.uk/pdf/supportnet/InternetSafety.pdf

Childnet International 'Know It All' CD
http://publications.teachernet.gov.uk

Family Online Safe Institute
www.fosi.org

Internet Watch Foundation
www.iwf.org.uk

Parents Centre
www.parentscentre.gov.uk

Internet Safety Zone
www.internetsafetyzone.com

Appendix 5:

<u>Internet Site Log Sheet</u>

Name: _____ Date:_____/_____/_____ Time: _____

Workstation (Location): _____

URL (Unique Resource Locator, i.e. website address):_____

_____

_____

☐ Tick box if URL printed & attached

Recommendation: Block site ☐   Unblock site ☐

* Once completed - pass this form to the ICT coordinator

For Technician's use only:

Southwark LEA - Tel: 0207 525 5000   Atomwide (ISP) - Tel:
                                                                - Fax:

Details of resolution: