



Online
Safety

January

2022

Key Details

Designated Safeguarding Leads	Laura Liddell (Head Teacher)
Designated Safeguarding Leads	Natalie Trewhella (Deputy Head/SENCo)
Designated Safeguarding Leads	Sarah Shaw (SLT)
Governor with lead responsibility	Tracy Davinson
Date written	January 2022
Date of next review	January 2023

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

1. Policy Aims

- This online safety policy has been written by Bloemfontein Primary School, involving staff, pupils, governors and parents/carers
- It takes into account, the DfE statutory guidance 'Keeping Children Safe in Education' 2021, Early Years and Foundation Stage 2017, 'Working Together to Safeguard Children' 2018 and the Durham Safeguarding Children's Partnership procedures.
- The purpose of Bloemfontein Primary School online safety policy is to:
 - Safeguard and protect all members of Bloemfontein Primary 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

Bloemfontein Primary School identifies that the issues classified within online safety 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

- Bloemfontein Primary School 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

- Bloemfontein Primary School identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life
- Bloemfontein Primary School 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, or where learners, staff or other individuals have been provided with setting issued devices for use off-site, such as a work laptops, tablets or mobile phones

Links with other policies and practices

This policy links with several other policies, practices and action plans including Anti-bullying policy, Acceptable Use Policies (AUP) and the Code of Conduct/Staff Behaviour policy, Behaviour policy, Child Protection/Safeguarding policy, Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE), Citizenship and Relationships and Sex Education (RSE), Data Protection and Photograph policy

3. Monitoring and Review

Technology in this area evolves and changes rapidly. Bloemfontein Primary School 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 other significant changes
- 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, Designated Safeguarding Leads (DSLs) will be informed of online safety concerns, as appropriate
- The named governor for safeguarding 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 (Laura Liddell) has lead responsibility for online safety. Whilst activities of the designated safeguarding lead may be delegated to an appropriately trained deputy, overall the ultimate lead responsibility for safeguarding and child protection, including online safety remains with the DSL.

- Bloemfontein Primary School recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

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/behaviour policy 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 the 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

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 setting's 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 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 (log on CPOMS)
- 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 setting's management team and Governing Body
- Work with the leadership team to review and update online safety policies on a regular basis (at least annually) with input from all stakeholders
- Meet regularly (termly) with the governor with a lead responsibility for safeguarding

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

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 DSL and leadership team (two factor authentication where appropriate, encrypted memory sticks/mac devices, Smoothwall filtering) to ensure that the setting's 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 deputy DLS to our filtering and monitoring systems, to enable them to take appropriate safeguarding action if/when required

It is responsibility of pupils (dependent on age and level of understanding):

- 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

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
- 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 Education and 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:
 - Ensuring education regarding safe and responsible use precedes internet access. Including online safety in Personal, Social, Health and Economic (PSHE), Relationships and Sex Education (RSE) and computing programmes of study. The teaching of online safety should follow the long and medium term plans put in place by leaders but should also be responsive to the needs of the children
 - Reinforcing online safety messages whenever technology or the internet is in use
 - Educating learners in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation
 - 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:
 - Displaying acceptable use posters in all rooms with internet access

- Informing learners that network and internet use will be monitored for safety and security purposes and in accordance with legislation
- Rewarding positive use of technology (dojos, opportunity to be digital leaders)
- 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 enhance and support our online safety curriculum

Supporting vulnerable learners

- Bloemfontein Primary School 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
- Bloemfontein Primary School 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, Bloemfontein Primary School will seek input from specialist staff

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 National Online Safety Training (online), annual staff meetings and ongoing professional development
- 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

Engagement with parents/carers

Bloemfontein Primary School recognises that parents and carers have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies

- We will build a partnership approach to online safety with parents and carers by:
 - Providing information and guidance on online safety in a variety of formats. This will include offering specific online safety awareness training and highlighting online safety at other events such as parent evenings, transition events, and sports days
 - Drawing their attention to the online safety policy and expectations in newsletters, letters, dojo messages, social media, parent's evening, 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

Bloemfontein Primary School recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid

pace

- We will:

- Regularly review the methods used to identify, assess and minimise online risks

- Examine emerging technologies for educational benefit and undertake appropriate risk assessments before 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

- 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 Classroom Use

- Bloemfontein Primary School 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

- Games consoles and other games-based technologies

- 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

- Smoothwall filtering - monitoring

-Quality-first teaching around searches, training on searching and physical monitoring

We will ensure that the use of internet-derived materials, by staff and learners, complies with copyright law and acknowledge the source of information

- Supervision of learners will be appropriate to their age and ability:

Early Years Foundation Stage and Key Stage 1 - Access to the internet will be by adult demonstration, with occasional directly supervised access to specific and approved online materials, which supports the learning outcomes planned for the learners' age and ability

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

Managing Internet access

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

Filtering and Monitoring

A guide for education settings about establishing 'appropriate levels' of filtering and monitoring can be found at: <https://www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/appropriate-filtering-and-monitoring>

- Bloemfontein Primary School governors and leaders have ensured that our setting has age and ability appropriate filtering and monitoring in place, to limit learners' 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
- 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 learners; effective classroom management and regular education about safe and responsible use is essential. Concerns must be reported to DSLs and logged on CPOMS

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.

Full information can be found in our Data Protection policy. (on website)

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 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

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.

- From Year 2 (Y1 to be given their own log in) 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:**

- Use strong passwords for access into our system

- Change their passwords regularly

- 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

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 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

Publishing Images and Videos Online

- We will ensure that all images and videos shared online are used in accordance with the associated policies, including (but not limited to) the cameras and image use, data security, acceptable use policies, codes of conduct/behaviour, social media and use of personal devices and mobile phones

Managing emails

- 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/behaviour policy.
- The forwarding of any chain messages/emails is not permitted
- Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email
- 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 tell headteacher if they receive offensive communication, and this will be recorded in our safeguarding files/records.

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, learners and parents
- Shared mailboxes will be monitored by relevant staff. Only necessary staff will have access

8. Social Media Expectations

- The expectations regarding safe and responsible use of social media applies to all members of Bloemfontein Primary School community
- The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger
- All members of Bloemfontein Primary School community are expected to engage in social media in a positive, safe and responsible manner

o All members of Bloemfontein Primary School 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

o The use of social media during school hours for personal use is permitted but only during designated break times and in the staff room or areas not occupied by pupils. 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. All staff must use their own internet and not be connected to the server

• Concerns regarding the online conduct of any member of Bloemfontein Primary School 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

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/behaviour policy as part of acceptable use policy

• 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

• 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 Bloemfontein Primary School 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 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

Pupils Personal Use of Social Media

- Safe and appropriate use of social media will be taught to pupils as part of a 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 pupils under this age
- Any concerns regarding 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
- 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 and how to report concerns both within the setting and externally

Official Use of Social Media

- Bloemfontein Primary School official social media channels are: twitter, facebook and class dojo

- The official use of social media sites only takes place with clear educational or community engagement objectives, with specific intended outcomes

o Leadership staff have access to account information and login details for our social media channels, in case of emergency, such as staff absence

- Official social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only

- Official social media use will be conducted in line with existing policies, including: antibullying, image/camera use, data protection, confidentiality and child protection

-All communication on official social media platforms will be clear, transparent and open to scrutiny

- Parents/carers and learners will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community

- Parents and carers will be informed of any official social media use with learners; written parental consent will be obtained, as required

Staff expectations

- Members of staff who follow and/or like our official social media channels will be advised to use dedicated professional 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:
 - Sign our social media 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, learners, parents and carers

 - Inform the DSLs of any concerns, such as criticism, inappropriate content or contact from learners

9. Use of Personal Devices and Mobile Phones

- Bloemfontein Primary School 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

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. All members of Bloemfontein Primary School 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 Bloemfontein Primary School community are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared

- Mobile phones and personal devices are not permitted to be used around children

- 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 Bloemfontein Primary School community are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or would otherwise contravene our behaviour or child protection policies

- All members of Bloemfontein Primary School community are reminded that taking covert images typically under clothing (Upskirting) is illegal and will be dealt with as part of the discipline policy

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:

- 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

- Not use personal devices during teaching periods, unless written permission has been given by the headteacher or Deputy Head, such as in emergency circumstances

- Ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations

- If a member of staff breaches our policy, action will be taken in line with our code of conduct/staff behaviour and allegations policy

- If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device, or have committed a criminal offence, the police will be contacted

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

- Bloemfontein Primary School expects learners' personal devices and mobile phones to be switched off and handed in to the school office on a morning where they will be logged and kept securely

- Learners are not permitted to wear SMART watches that can connect to a mobile phone for messages/phone calls. A simple fitness tracker or wrist watch can be worn

- If a learner needs to contact his/her parents or carers they will be allowed to use the school office phone and parents are advised to contact their child via the main office

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, behaviour, child protection and image use
- 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 of any breaches our policy.

10. Responding to online safety concerns

All members of the community will be made aware of the reporting procedure for online safety concerns

- All issues must be reported on our recording system, CPOMS and tagged as online safety
- All members of the community must respect confidentiality and the need to follow the official procedures for reporting concerns. Learners, parents and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure
- We require staff, parents, carers and learners to work in partnership 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 Team
- Where there is suspicion that illegal activity has taken place, we will contact the Education Safeguarding Team or Durham 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 DSLs will speak with Durham Police first to ensure that potential investigations are not compromised

Staff Misuse

- Any complaint about staff misuse will be referred to the headteacher 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.

11.Procedures for Responding to Specific Online Incidents or Concerns Online Sexual Violence and Sexual Harassment between Children

Bloemfontein Primary School 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 child protection and anti-bullying policy

- Bloemfontein Primary School recognises that the internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities
- Bloemfontein Primary School also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online
- Bloemfontein Primary School 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 by implementing a

range of age and ability appropriate educational methods as part of our PSHE and RSE curriculum. It will also be included in workshops delivered to staff and parents

- 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.

Cyberbullying

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

Online Hate

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at Bloemfontein Primary School and will be responded to in line with existing policies, including anti-bullying and behaviour
- All members of the community will be advised to report online hate in accordance with relevant policies and procedures
- The Police will be contacted if a criminal offence is suspected
- If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL (or deputy) will obtain advice through First Contact or Durham Police

Online Radicalisation and Extremism

- We will take all reasonable precautions to ensure that learners and staff are safe from terrorist and extremist material when accessing the internet on site. (Smoothwall and physical monitoring are always in place)
- If we are concerned that a child or parent/carer may be at risk of radicalisation

online, the DSL (or deputy) 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 DSL (or deputy) will be informed immediately, and action will be taken in line with the child protection and allegations policies