



BANTOCK PRIMARY SCHOOL

Digital Safeguarding Policy

Headteacher	
Chair of Governors	
Approved Date	02.02.2017/31.01.2019/24.6.20/31.3.21/2.2.22/1.2.23/31.1.24

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 Digital Safeguarding Lead
 - 4.3 Members of staff
 - 4.4 Staff who manage the technical environment
 - 4.5 Digital Ambassadors
 - 4.6 Learners
 - 4.7 Online Safety Group
 - 4.8 Parents
 5. Education and Engagement Approaches
 - 5.1 Education and engagement with learners
 - 5.2 Vulnerable Learners
 - 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 Firewall, Filtering and Monitoring
 - 7.4 Managing Personal Data Online
 - 7.5 Cyber 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 Management of Learning Platforms
 - 7.10 Management of Applications (apps) used to Record Learners Progress
 - 7.11 Remote Learning
 - 7.12 Management of Artificial Intelligence
 8. Social Media
 - 8.1 Expectations
 - 8.2 Staff Personal Use of Social Media
 - 8.3 Learners Personal Use of Social Media
 - 8.4 Official Use of Social Media
 9. Mobile Technology: Use of Personal Devices and Mobile Phones
 - 9.1 Expectations
 - 9.2 Staff Use of Personal Devices and Mobile Phones
 - 9.3 Learners 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 learner online behaviour and/or welfare
 - 10.2 Concerns about staff online behaviour and/or welfare
 - 10.3 Concerns about parent/carer online behaviour and/or welfare
 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 abuse and exploitation (including child sexual abuse and sexual or criminal exploitation)
 - 11.4 Indecent Images of Children (IIOC)
 - 11.5 Cyberbullying
 - 11.6 Online Hate
 - 11.7 Online Radicalisation and Extremism
 - 11.8 Online Challenges and Hoaxes
- Responding to an Online Safety Concern Flowchart
- Useful Links for Educational Settings

1 Policy aims

- This online safety policy has been written by Bantock Primary School, involving staff, learners and parents/carers, building on the Kent County Council/The Education People online safety policy template, with specialist advice and input as required.
- It takes into account the DfE statutory guidance '[Keeping Children Safe in Education](#)' 2023, [Early Years and Foundation Stage](#) 2017 '[Working Together to Safeguard Children](#)'
- The purpose of Bantock Primary School online safety policy is to
 - safeguard and promote the welfare of all members of Bantock Primary School community online.
 - identify approaches to educate and raise awareness of online safety throughout our 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 follow when responding to online safety concerns.
- Bantock Primary School identifies that the issues classified within online safety are considerable but can be broadly categorised into four 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.
 - **Commerce:** online interactions that involve financial transactions and agreements.

2 Policy scope

- Bantock Primary School recognises 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 (see *Keeping Children Safe In Education*)
- Bantock 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 which present positive and exciting opportunities, as well as challenges and risks. Such risks have been classified within *Keeping Children Safe in Education* to Content, Contact, Conduct and Commerce - the 4 Cs.
- Bantock Primary School will empower our learners to acquire the knowledge needed to use the internet and technology in a safe, considered and respectful way, and develop their resilience so they can manage and respond to online risks.
- This policy applies to all staff, including the governing board, 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 and parents and carers.
- This policy applies to all access to the internet and use of technology, including mobile technology, or where learners, staff or other individuals have been provided with setting issued devices for use, both on and off-site.

2.2 Links with other policies and practices

- This policy links with several other policies, practices and action plans, including but not limited to:

- Anti-bullying policy
- Acceptable and Responsible Use Policies
- **Staff Code of Conduct and Staff Handbook**
- Rights Respecting Behaviour
- Safeguarding & Child Protection
- **Technology Policy**
- Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE), Citizenship and Relationships and Sex Education (RSE)
- Data Protection GDPR Policy

3 Monitoring and review

- Technology evolves and changes rapidly; as such Bantock Primary School will review this policy at least annually. The policy will be revised following any national or local policy updates, any local child protection concerns and/or any changes to our 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/or Safeguarding Leads** will be informed of online safety concerns, as appropriate.
- The Safeguarding Lead Governor will report on online safety practice and incidents, including outcomes, on a regular basis to the wider governing **board**.
- Any issues identified via monitoring policy compliance will be incorporated into our action planning.

4 Roles and Responsibilities

- The Designated Safeguarding Leads (DSL) are Mrs H Sarai and Mr J Thomas who have overall lead over safeguarding in school. The Deputy DSL's are Mrs R McEntee and Mr D Fullard. DSLs and Deputy DSLs all have appropriate Safeguarding Training and they are the ultimate lead responsibility for safeguarding and child protection, including online safety.
- The Digital Safeguarding Manager (DSM), Mr D Fullard is recognised as holding overall lead responsibility for online safety. Online safety activities may be delegated from the DSLs to the DSM. The DSM holds the European Pedagogical ICT Online Safety Awareness Certificate (EPICT), which marks a commitment to keeping young children safe online.
- Bantock Primary School recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

4.1 The Leadership Team will:

- Create a whole setting culture that incorporates online safety throughout all elements of Bantock life.
- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Implement appropriate and up-to-date policies regarding online safety which addresses the acceptable use of technology, peer on peer abuse, use of social media and mobile technology, reviewing these at least annually and where required (new technology, guidance etc).
- Work with technical staff and IT support, Concero, to ensure that suitable and appropriate filtering and monitoring systems are in place.
- Support the DSLs and any deputies by ensuring they have enough time and resources to carry out their responsibilities.
- Ensure robust reporting channels are in place for the whole community to access regarding online safety concerns.

- Undertake appropriate risk assessments regarding the safe use of technology on site.
- Audit and evaluate online safety practice to identify strengths and areas for improvement.
- Ensure that staff, learners and parents/carers are proactively engaged in activities which promote online safety.
- Support staff to ensure that online safety is embedded within a progressive whole setting curriculum which enables all learners to develop an appropriate understanding of online safety.

4.2 The Digital Safeguarding Manager will:

- Act as a named point of contact within the setting on all online safeguarding issues.
- Liaise with other members of staff, IT technicians, network managers and the SENCO on matters of online safety.
- Ensure appropriate referrals are made to relevant external partner agencies, as appropriate.
- Work alongside DSLs to ensure online safety is recognised as part of the settings safeguarding responsibilities, and that a coordinated whole Bantock Primary School approach is implemented.
- 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.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and child protection training.
- 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.
- Monitor online safety incidents, **including filtering and monitoring reports**, to identify gaps and trends and use this data to update the education response and Bantock Primary School policies and procedures.
- Maintain records of online safety concerns, as well as actions taken, as part of the settings safeguarding recording mechanisms.
- Report online safety concerns, as appropriate, to the DSLs, the leadership team and Governing **board**.
- Work with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input.
- Meet regularly with the governor with a lead responsibility for safeguarding.
- Meet termly with an Online Safety group to give all members of the school community an opportunity to voice their opinions and concerns about school and home-related technology use.
- Use the 360 Online Safe audit tool to baseline and review online safety at Bantock Primary School.
- Monitor Safeguarding Concerns through **Surf Protect filtering reports and Senso monitoring** reports and other channels, reporting the information to Designated Safeguarding Leads to discuss outcomes, and reporting data to governors.

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

- Contribute to the development of our online safety policies.
- Read and adhere to our online safety policy and acceptable use of technology policies.
- Take responsibility for the security of IT systems and the electronic data they use or have access to.
- Model good practice when using technology with learners.

- 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, **gaining an understanding of pupils current knowledge and risk factors and providing the support to develop resilience and overcome these issues.**
- Have an awareness of a range of online safety issues and how they may be experienced by the learners in their care.
- Identify online safety concerns and take appropriate action by following the Bantock Primary School safeguarding policies and procedures.
- Know when and how to escalate online safety issues, including reporting to the DSL.
- **Understanding the routes to reporting and signposting** learners and parents/carers to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.
- Not following the explicit expectations for maintaining a secure school environment could result in disciplinary actions.
- **Display and share the Digital 5 a Day (Appendix B) to promote healthy technology use.**

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

- Provide technical support and perspective to the DSM and Bantock Primary School leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Implement appropriate security measures including **multi-factor authentication**, encrypted learning platform and bitlocker passwords as directed by the leadership team to ensure that the settings IT infrastructure is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensure that our filtering policy and monitoring systems and approaches are applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- **Keep systems up to date with security patches and installed with appropriate virus protection.**
- Ensure appropriate technical support and access to our filtering and monitoring systems is given to the DSL's and/or deputies to enable them to take appropriate safeguarding action when required.

4.5 Digital Ambassadors

The Digital Ambassadors are 12 pupils selected at the start of Year 5 who may have shown positive attributes in using technology and with supportive or mentoring qualities. These pupils are trained regularly throughout Year 5 with Wider Learning in order to support pupils across school with Digital Safety. They continue to hold their responsibility into Year 6 and are trained as Digital Ambassadors Plus, gaining additional responsibility and taking greater ownership.

It is the responsibility of Digital Ambassadors to:

- Take part in regular training sessions during their time as Digital Ambassadors in Year 5 and 6.
- Act as role models for safe and responsible use of technology.
- Promote ways to stay safe online and when using technology.
- Explain the risks involved when using technology.
- Ensure that they adhere to a code of conduct and share a digital charter of their own.
- Support others with problems, issues or concerns and alert appropriate adults to serious concerns.

(developed and agreed by 2021-22 Digital Ambassadors)

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

- Engage in age/ability appropriate online safety education.
- Contribute to the development of online safety policies.
- Read and adhere to the acceptable use of technology and behaviour policies.
- Respect the feelings and rights of others, on and offline.
- Take an appropriate level of responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if they are concerned about anything, they or others experience online.
- **Have some understanding of the routes to reporting available.**
- **Follow the Digital 5 a Day (Appendix B) steps that promote a healthy lifestyle that includes technology.**

4.7 It is the responsibility of the Online Safety group to:

- Act on behalf of the school community, including the staff, pupils, parents, governors and leadership team, as well as the wider community to voice concerns and issues related to technology.
- Meet termly to share knowledge and practice.
- Work collaboratively to address concerns in line with school policy.
- Develop existing tools and policy such as the Acceptable Use Policy and Pupil Survey.
- Review the curriculum to align with current pupil needs and concerns.
- Feedback information to the wider community.

4.8 It is the responsibility of parents and carers to:

- Read our acceptable use of technology 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, **which are shared through a variety of means including the school website, social media and newsletters.**
- Role model safe and appropriate use of technology and social media and abide by the home-school agreement *and* acceptable use of technology policies.
- Seek help and support from the Bantock Primary School or other appropriate agencies, if they or their child encounter online issues.
- Contribute to the development of our online safety policies.
- Use our systems, such as learning platforms and other IT resources, safely and appropriately.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by the new and emerging technologies that their children access and use at home.

5. Education and engagement approaches

Bantock Primary School takes proactive steps to **educate and raise awareness** of online safety within its community as this is crucial to mitigating risks. Here are some key approaches:

- **Curriculum Integration:** Online safety is **integrated into the curriculum**, ensuring that learners receive age-appropriate education on topics such as privacy, cyberbullying, and responsible internet use.
- **Assemblies and Workshops:** Regular **assemblies and workshops** are conducted to discuss online safety. These sessions cover topics like identifying risks, reporting concerns, and promoting positive digital behaviour.
- **Parent and Carer Engagement:** Bantock Primary involves parents and carers through **information sessions, workshops, and newsletters**. They receive guidance on monitoring their child's online activities and setting appropriate boundaries. Bantock runs a yearly Digital Protector Course for parents to support them in keeping their children safe online, recognising risks and where to go for support.

- **Guest Speakers and Experts:** Bantock invites **guest speakers and experts** to address learners, staff, and parents. These professionals share insights, best practices, and real-life examples related to online safety.

Bantock recognises that fostering a culture of **open communication** and encouraging everyone to be **digitally vigilant** are essential components of Bantock Primary School's commitment to online safety.

5.1 Education and engagement with learners

- The setting will establish and embed a whole Bantock Primary School culture and will raise awareness and promote safe and responsible internet use amongst learners by:
 - ensuring our curriculum and whole Bantock Primary School approach is developed in line with the UK Council for Internet Safety (UKCIS) '[Education for a Connected World Framework](#)' and DfE '[Teaching online safety in school](#)' guidance.
 - ensuring online safety is addressed in Relationships Education, Relationships and Sex Education, Health Education, Citizenship and Computing programmes of study. For this, the 'Education for A Connected World' framework statements have been mapped out throughout the school's PDR scheme, Jigsaw, with some standalone sessions being taught within computing, where it is not possible to do this within PSHE.
 - **Content linked to 'Education for a Connected World' is taught using ProjectEVOLVE online resources that promote discussion. Knowledge is checked using Knowledge Maps prior to a theme and this is used to drive the learning required.**
 - **Further opportunities to support online safety Education are planned for, including Chatter Sessions, which take place termly in Year 4 to 6 in gender separated classrooms where pupils can openly and honestly discuss issues that are important to them. See PDR Policy.**
 - reinforcing online safety principles in other curriculum subjects as appropriate, and whenever technology or the internet is used on site.
 - Developing a group of pupils whom are trained with digital safety knowledge as Digital Ambassadors.
 - implementing appropriate peer education approaches, for example, sessions created by Digital Ambassadors to present in assemblies.
 - creating a safe environment in which all learners feel comfortable to say what they feel, without fear of getting into trouble and/or being judged for talking about something which happened to them online.
 - involving the DSM as part of planning for online safety lessons or activities, so they can advise on any known safeguarding cases, and ensure support is in place for any learners who may be impacted by the content.
 - making informed decisions to ensure that any educational resources used are appropriate for our learners.
 - using external visitors, including the Online Behaviours team and PCSOs where appropriate, to complement and support our internal online safety education approaches
 - providing online safety education as part of the transition programme across the key stages and/or when moving between establishments.
 - rewarding positive use of technology.
 - **providing opportunities for pupils who misuse technology to reflect on the risks associated with the concern.**
 - **Including the correct terminology for pupils to explore and understand as part of the 4 Cs / Areas of risk and positive use of technology (promoted with Digital 5 a Day - Appendix B)**

- Bantock Primary School will support learners to understand and follow our acceptable use policies in a way which suits their age and ability by:
 - displaying acceptable use posters in rooms with internet access.
 - informing learners that network and internet use will be monitored for safety and security purposes, and in accordance with legislation.
 - seeking learner voice when writing and developing online safety policies and practices, including curriculum development and implementation.
 - discussing the background of the Acceptable and Responsible Use Policy.
- Bantock Primary School will ensure learners develop the underpinning knowledge and behaviours needed to navigate the online world safely, in a way which suits their age and ability by:
 - ensuring age appropriate education regarding safe and responsible use precedes internet access through ProjectEvolve and further resources,
 - teaching learners to evaluate what they see online and recognise techniques used for persuasion, so they can make effective judgements about if what they see is true, valid or acceptable (**misinformation and disinformation**)
 - educating them in the effective use of the internet to research, including the skills of knowledge location, retrieval and evaluation (**Search Coach**).
 - enabling them to understand what acceptable and unacceptable online behaviour looks like.
 - preparing them to identify possible online risks and make informed decisions about how to act and respond.
 - ensuring they know how and when to seek support if they are concerned or upset by something they see or experience online.

5.2 Vulnerable Learners

- Bantock Primary School recognises that any learner can be vulnerable online, and vulnerability can fluctuate depending on their age, developmental stage and personal circumstances. However, there are some learners, for example looked after children and those with special educational needs, who may be more susceptible or may have less support in staying safe online.
- Bantock Primary School will ensure that differentiated and appropriate online safety education, access and support is provided to vulnerable learners.
- Staff at Bantock Primary School will seek input from specialist staff as appropriate, including the DSM and SENCO to ensure that the policy and curriculum is appropriate to our community's needs.

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 which is integrated, aligned and considered as part of our overarching safeguarding approach. This is included within the annual safeguarding training and as a standalone training session. The standalone Digital Safeguarding session is delivered by the DSM and/or external companies (Concerto, Online Behaviours)
 - Staff training covers the potential risks posed to learners (content, contact, conduct, commerce) as well as our professional practice expectations.
 - build on existing expertise by provide opportunities for staff to contribute to and shape our online safety approaches, including curriculum, 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, including personal use of social media, can have an impact on their professional role and reputation.
- highlight useful educational resources and tools which staff could use with learners.
- ensure all members of staff are aware of the procedures to follow regarding online safety concerns involving learners, colleagues or other members of the community.

5.4 Awareness and engagement with parents and carers

- Bantock 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 includes the dissemination of information at parents evenings, the opportunity to join chatter sessions with a Parent Ambassador, information sharing on the school website and social media platform, as well as directing them to learning content, for example free workshops and classes.
 - drawing their attention to our Digital Safeguarding policy and expectations in our newsletters and other external communication (such as letters and social media channels) as well as in our prospectus and on our website.
 - requesting parents and carers read online safety information as part of joining our community, for example, within our home school agreement.
 - Requesting parents to read our Responsible and Acceptable Use Policy and discuss the implications with their children.
 - **Members of the parental community are also involved with the Online Safety group, which gives them an opportunity to voice opinions and concerns, whilst discussing current technology issues regarding school.**
 - **Parent chatter sessions and a Digital Protector course have been established to support parents with their understanding of keeping their children safe online.**

6 Reducing Online Risks

- Bantock Primary School recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace, **as well as an increase in time accessed and exposed to due to Home Learning and the provision of 1 to 1 devices for KS2 pupils.**
- We will
 - regularly review the methods used to identify, assess and minimise online risks.
 - This includes KS-2 pupils completing an online safety survey to identify what risks are greater for our pupils currently.
 - Examine emerging technologies for educational benefit and undertake appropriate risk assessments before their use in the Bantock Primary School is permitted.
 - ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that access is appropriate.
 - recognise that due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via our systems or devices and as such identify clear procedures to follow if breaches or concerns arise.
- 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. This is clearly outlined in our acceptable use of technology policies and highlighted through a variety of education and training approaches. The school also has implemented Rules for Home Learning, which includes aspects of internet safety as part of online lessons.

7. Safer Use of Technology

7.1 Classroom use

- Bantock Primary School uses a wide range of technology. This includes access to
 - Computers, laptops, tablets and other digital devices
 - Internet, which may include search engines and educational websites
 - Learning apps
 - Learning platform (Office 365/**Teams**)
 - Email
 - Games consoles and other games-based technologies
 - Digital cameras, web cams and video cameras
- All setting owned devices will be used in accordance with our acceptable use of technology policies and with appropriate safety and security measures in place.
- Members of staff will always evaluate websites, (particularly YouTube), tools and apps fully before use in the classroom or recommending for use at home. The school home page, 'Square One' for pupils is managed by Concero and uses Kiddle Search with safety features enables.
- The setting will use appropriate search tools as identified following an informed risk assessment (Kiddle). Other suggested tools for pupils to use are [SWGfL Swiggle](#), [Dorling Kindersley Find Out](#). Using Kiddle ensures that pupils are exposed to a Google like structure that can be used as a discussion point for real life situations.
- **Unsafe searches are blocked instantly through keywords blacklisted with Surf Protect.**
- 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 internet access and technology use will be appropriate to learners age and ability.
 - **Early Years Foundation Stage and Key Stage 1**
 - Appropriate apps are accessed independently. 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.

7.2 Managing internet access

- We will maintain a written record of users who are granted access to our devices and systems, including Wi-Fi.
- All staff, learners and visitors will read and agree A Responsible and Acceptable Use Policy before being given access to our computer system, IT resources or the internet.

7.3 Virus Protection, firewalls, filtering and monitoring

7.3.1 Decision making

- Bantock Primary School governors and leaders have ensured that our school has age and ability appropriate filtering and monitoring in place to limit learner’s exposure to online risks.
- 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.
- **Filtering and monitoring procedures will be reviewed at least annually, or when required (an identified safeguarding risk, new technology, guidance etc) with members of the leadership team with safeguarding and technical expertise and IT support.**
- The headteacher receives emails of blocked searches which are analysed by the DSM
- The leadership team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.
- The governors and leaders are mindful to ensure that “over blocking” does not unreasonably restrict access to educational activities and safeguarding materials.
- 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.

7.3.2 Appropriate filtering

- Bantock Primary School’s education broadband connectivity is provided through **Exa Networks**
- Bantock Primary School uses **Exa Network Surf Protect** Filtering
 - **Exa Network Surf Protect** Filtering blocks access to sites which could promote or include harmful and/or inappropriate behaviour or material. This includes content which promotes discrimination or extremism, drugs/substance misuse, malware/hacking, gambling, piracy and copyright theft, pro-self-harm, eating disorder and/or suicide content, pornographic content and violent material.
 - **Exa Network Surf Protect** Filtering is a member of [Internet Watch Foundation](#) (IWF) and blocks access to illegal Child Abuse Images and Content (CAIC).
 - **Exa Network Surf Protect** Filtering integrates the ‘the police assessed list of unlawful terrorist content, produced on behalf of the Home Office’ **and confirms that filters for illegal content cannot be disabled by school.**
- We work with Concerro to ensure that our filtering policy is continually reviewed to reflect our needs and requirements.
- If learners or staff discover unsuitable sites or material, they are required to report it to a member of staff immediately.
- Filtering breaches will be reported to the DSM and technical staff and will be recorded and escalated as appropriate.
- Parents/carers will be informed of filtering breaches involving learners as appropriate.
- Any access to material believed to be illegal will be reported immediately to the appropriate agencies, such as the IWF, the police and/or CEOP.

7.3.2.1 Appropriate Firewalls

- **Exa uses a hosted FortiGate VM firewall to analyse incoming and outgoing data and blocks traffic that is considered to be a threat.**
- **Configurations and updates are hosted remotely by Exa**

7.3.2.2 Appropriate Virus Protection

- **Windows Defender is in place across school as virus protection and Anti-Malware whereby files and sites are scanned preventing access to malicious content.**
- **Windows Defender is updated automatically to provide real time detection and prevention.**

7.3.3 Appropriate monitoring

- We will appropriately monitor internet use on all setting owned or provided internet enabled devices. This is achieved by:
 - e.g. physical monitoring (supervision)
 - monitoring internet and web access (reviewing logfile information)
 - Senso technology monitoring services are being used as a deeper filtering service to use with pupils having their own login IDs.
 - **Exa Networks Quantum+ monitoring through the Surf Protect portal.**
- 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.
- Concerns and violations are recorded by the DSM on a tracking sheet during regular monitoring and categorised in order to identify solutions.
- Violations and the outcomes of this are discussed with DSLs and information reported to governors.
- If a concern is identified via monitoring approaches we will respond in line with the Safeguarding and Child Protection policy.

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.
 - Full information can be found in our information security policy which can be accessed at GDPR Statement on the School Website or within the policy on the Learning Platform.

7.5 Cyber security and management of information systems

*For detail, refer to the **Cyber Security Policy and Cyber Response Plan***

- A cyber security breach is the unauthorised access to data, systems and networks which may be caused by:
 - Email mishaps
 - Phishing attacks
 - Human error
 - Intentional liabilities
- We take appropriate steps to ensure the security of our information systems **and preventions of cyber security breaches**, including:
 - **Identifying those that have access to the most sensitive information.**
 - **Training staff about Cyber Crime Risks regularly, including annual National Cyber Security Centre training.**
 - **Self and external audits to identify actions to address, if required.**
 - Supporting pupils in understanding their role in cyber security.
 - Virus protection being updated regularly.
 - Keeping software up to date.
 - All data is kept in line with the data protection policy.
 - 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.
 - No portable storage media are allowed.
 - Not downloading unapproved or unlicensed software to work devices or opening unfamiliar email attachments.
 - Deleting unused or unnecessary software.

- Preventing, as far as possible, access to websites or tools which could compromise our systems, including anonymous browsing and other filtering bypass tools eg disabling proxy in school.
- Checking files held on our network, as required and when deemed necessary by leadership staff.
- The appropriate use of user logins and passwords to access our network.
 - Specific user logins and passwords will be enforced for all users.
 - Multi factor authentication used, where possible (must include Microsoft)
- All users are expected to log off or lock their screens/devices if systems are unattended.
- Users only accessing data that they have the right to access.
- Concero upholding stringent security checks of the systems as part of their ongoing audit.
- Secure Schools completing an external audit of all systems and support policy building.
- Concero managing backups of secure data and monitor this.
- Following Emergency and Disaster Policy in the event of a Cyber Security Attack.
- Removing old users from systems promptly.
- A list of approved technologies and password management is found in Appendix C.
- As part of the school's compliance for membership in the Risk Protection Arrangement (RPA), Bantock adheres to Conditions of Cover. These are that:
 - Bantock has regular offline backups for any non-cloud based servers (currently SIMS - FMS) - ideally in multiple locations. Cloud based clients should have valid credentials that state their backup policy.
 - All staff must receive the National Cyber Security Centre's training. This is delivered as part of annual Safeguarding and GDPR training.
 - The school is registered with Police CyberAlarm.
 - A Cyber Response Plan is in place, which works alongside the Emergency and Disaster Policy as a response in the event of a cyber incident.

7.5.1 Password policy

- All members of staff 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.
- From Reception, all pupils are provided with a unique school email address and password to access Microsoft Office 365. Learners are responsible for keeping their password private.
- We require all users to
 - use strong passwords for access into our system and resources - this is an unlimited length but a MINIMUM of 8 characters and with a recommendation of 3 random words and numbers for passwords.
 - Use Multi Factor Authentication where possible (must include Microsoft)
 - Where Single Sign in through Microsoft is available, MFA will support the security of this.
 - Change passwords regularly
 - change their passwords if they suspect it has been compromised.
 - not share passwords or login information with others or leave passwords/login details where others can find them.
 - not to login as another user at any time.
 - lock access to devices/systems when not in use.
 - Check your password strength <https://www.security.org/how-secure-is-my-password/>
 - When training staff about Cyber Security, Passwords and Social Media, it is advised to them that personal accounts should be set up in a similar method (different and strong

passwords, MFA) so minimize the risk of compromised personal items which could lead to compromised school systems.

7.6 Managing the safety of our website

- We will ensure that information posted on our website meets the requirements as identified by the DfE. This is audited termly by the DSM/**Technology Lead**
- 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 learner'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.
- Studio Website has the responsibility for upholding the data and security of the school website, including the back up of it.

7.7 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 policies.
- Parents indicate within the General Consent form completed online what forms of publishing they consent to and this is updated yearly, or sooner if any changes occur.
- **The choices for permissions are within school circulation, external circulation to other parents/newspaper, and use on school's social media.**

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 of technology policies and the code of conduct/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. Staff should only use recognised school email systems in relation to work.
- Setting email addresses and other official contact details will not be used to set up personal social media accounts.
- Members of the community will immediately tell the DSLs 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.
- We have a Happy and Worry Box on the school website for pupils to contact the Headteacher with concerns. These messages are monitored by the DSLs and DSM to address any concerns. Any messages that are received that are offensive will be dealt with in line with school policy.

7.8.1 Staff email

- All members of staff are provided with an email address to use for all official communication; the use of personal email addresses by staff for any official business is not permitted.

- 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.

7.8.2 Learner email

- Learners use their email address to access Microsoft Teams and Office 365. However, settings are in place to prevent them from using this to send and receive emails and accessing content they do not have permissions to use.

7.9 Management of learning platforms

- Bantock Primary School uses Office 365 as its official learning platform.
- Concero manage the Bantock Primary School learning platform.
- Leaders and staff will regularly monitor the usage of the Learning Platform (LP), including message/communication tools and publishing facilities.
- Only current members of staff will have access to the LP.
- When staff leave the setting, their account will be disabled or transferred to their new establishment.
- Learners 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 learner's parents/carers may be informed.
 - If the content is illegal, we will respond in line with existing child protection procedures.
- Learners may require editorial approval from a member of staff. This may be given to the learner to fulfil a specific aim and may have a limited time frame.
- A visitor may be invited to view and/or edit a document on the platform, which will only be accessible to them through a personal link.

7.10 Management of applications (apps) used to record children's progress

- We use Evidence Me to track learners progress in EYFS, as well as practical activities in KS1 and KS2 and share appropriate information with parents and carers.
- The DSM will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that use takes place in accordance with data protection legislation, including the General Data Protection Regulations (GDPR) and Data Protection legislation.
- To safeguard learner's data
 - only learner issued devices will be used for apps that record and store learners' personal details, attainment or photographs.
 - Staff must not use personal devices whilst in the company of pupils
 - personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store learners' 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.

7.11 Remote Learning

- If staff are working from home providing Remote Learning, they must continue to abide by the Responsible and Acceptable User Policy as well as ensuring greater considerations to the risks involved with being in their own home, as well as pupils being in their home. For this reason, it is important for both staff and pupils to ensure that they are in an appropriate work space.
- Due to the nature of interactive lessons, pupils and staff may be seen on camera and microphones and speakers may be active. For this reason, safeguarding and privacy procedures must be closely adhered to for both staff and learners. This includes ensuring that personal information is not discussed and all communications are appropriate.
- Filtering systems continue to be in place when staff are engaging in Remote Learning.
- Where pupils have borrowed devices from school, these also have appropriate filtering in place.
- Staff must only use school devices to deliver Remote Learning.
- Settings are in place to ensure that staff are unable to make direct contact with pupils through email or messages and that this can only be done in a group (the class Team) or within usual school communication methods to parents (**Arbor messaging**, phone calls, Class Dojo).
- Usual reporting procedures for Safeguarding concerns are in place when Remote Learning.
- Up to date information supporting safe remote teaching and learning can be found at <https://swgfl.org.uk/resources/safe-remote-learning/>

7.12 Management of Artificial Intelligence (AI)

- Technology Manager will signpost safe and acceptable uses of Artificial Intelligence (AI) for school use (See Technology Policy)
- Users should always review and critically assess outputs from AI tools before submission or dissemination. Users should never rely solely on AI-generated content without review.
- All users must be aware that AI-generated content may possess biases, misinformation or inaccuracies. Users must always verify AI-produced results using trusted sources before considering them in academic work.
- Users must not use AI tools to create or propagate harmful, misleading, or inappropriate content ensuring safety and respect at all times.
- Any use of AI to aid assignments, projects, or research must be declared with full transparency, sources should be included.
- AI tools will be used for educational purposes only. Misuse or malicious use of AI technologies will lead to disciplinary action.
- AI tools must be age appropriate (Many AI chatbots are for over 13s and under 18s must have permission).
- Information inputted into AI must be in line with GDPR compliance and uphold privacy (see GDPR Policy). Microsoft AI tools (e.g. CoPilot, Bing Chat) do not use organisational data that is inputted to train the model and it is protected, whereas others do may use data that is inputted.
- Due to the difficulty in filtering generative AI (evolution, variability of content, adversarial generation bypassing and user workaround), educators must be fully aware of the risks, capabilities and limitations at all times and educate pupils. AI usage, if appropriate, must be supervised with digital literacy skills and open conversations permeating the activity.

8. Social Media

8.1 Expectations

- The expectations' regarding safe and responsible use of social media applies to all members of Bantock 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 Bantock Primary School community are expected to engage in social media in a positive and responsible manner.
 - All members of Bantock Primary School community are advised not to post or share content that may be considered threatening, hurtful or defamatory to others on any social media service.
- We will control learner and staff access to social media whilst using Bantock Primary School provided devices and systems on site.
 - The use of social media during school hours, including teaching and PPA, for personal use is not permitted for staff.
 - The use of social media during school hours for personal use *is not* permitted for learners.
- Concerns regarding the online conduct of any member of Bantock Primary School community on social media, will be reported to the DSL's and be managed in accordance with our Staff Code of Conduct, 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 media 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 Staff Code of Conduct, Acceptable and Responsible User Policy and Social Media 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 school.
 - 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 services. 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 appropriate privacy levels on their personal accounts/sites.
 - Being aware of the implications of using location sharing services.
 - Opting out of public listings on social networking sites.
 - Logging out of accounts after use.
 - Using strong passwords.
 - Ensuring staff do not represent their personal views as being that of the setting.
- Members of staff are advised not to identify themselves as employees of Bantock Primary School on their personal social networking accounts; this is to prevent information 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. Staff are expected 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.

8.2.2 Communicating with learners and parents/carers

- Staff will not use personal social media accounts to contact learners or parents/carers, nor should any contact be accepted.
- All members of staff must not communicate with or add any current or past learners or their family members, as ‘friends’ on any personal social media sites, applications or profiles.
- Any pre-existing relationships or exceptions which compromise this requirement will be discussed with the DSL and the Headteacher.
 - Decisions made and advice provided in these situations will be formally recorded in order to safeguard learners, the setting and members of staff.
- If ongoing contact with a pupil is needed once a pupil has left the setting, it will be through school office communication between Bantock and the pupil’s current school.
- Any communication from learners and parents received on personal social media accounts will be reported to the DSL (or deputy) and headteacher.

8.3 Learners 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 are not permitted for use by children under the age of 13, or in some cases higher. This will be taught as part of Online Safety education and any reports of pupils using social media under the age of permission will be reported to DSLs and DSM and monitored.
- Any concerns regarding learners use of social media will be dealt with in accordance with existing policies, including anti-bullying and behaviour.
- Concerns regarding learners use of social media will be shared with parents/carers as appropriate, particularly when concerning underage use of social media services and games.
- Learners will be advised:
 - to consider the benefits and risks of sharing personal details or information 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 appropriate adults’ permission, and to only do so 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 on social media, both within the setting and externally.

8.4 Official use of social media

- Bantock Primary School official social media channels is:
 - [Twitter; www.Twitter.com/BantockSchool](https://twitter.com/BantockSchool)

- [Facebook; https://www.facebook.com/Bantock-Primary-School-109055535178986](https://www.facebook.com/Bantock-Primary-School-109055535178986)
- The official use of social media sites by Bantock Primary School only takes place with clear educational or community engagement objectives and with specific intended outcomes.
 - The official use of social media as a communication tool has been formally risk assessed and approved by the DSM/Computer Manager.
 - 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 accounts for official educational or engagement purposes only.
 - Official social media sites are suitably protected and is linked to the school 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 but not limited to anti-bullying, image/camera use, data protection, confidentiality and child protection.
- All information for communication on official social media platforms will be shared with the Computing Manager by staff to ensure that it is 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.
 - Only social media tools which have been risk assessed and approved as suitable for educational purposes will be used.
 - Any official social media activity involving learners will be moderated if possible.
- Parents and carers will be informed of any official social media use with learners; **if social media consent to photos has not been obtained on induction**, written parental consent will be obtained, as required.
- We will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

8.4.1 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 Responsible and Acceptable Use Policy.
 - Follow the Staff Code of Conduct
 - Be aware they are an ambassador for the setting.
 - Be professional, 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 appropriate consent has been given 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 private/direct messaging with current or past learners or parents/carers.
 - Inform the DSL (or deputy) and/or the headteacher of any concerns, such as criticism, inappropriate content or contact from learners.

9. Mobile Technology: Use of Personal Devices, Mobile Phones, Smart Watches

- Bantock Primary School recognises that personal communication through mobile technologies is part of everyday life for many learners, staff and parents/carers. Mobile technology needs to be used safely and appropriately within the setting.

9.1 Expectations

- All use of mobile technology including mobile phones and personal devices such as tablets, games consoles and wearable technology (including Smart Watches) will take place in accordance with our policies, such as anti-bullying, behaviour and child protection and with the law.
- Electronic devices of any kind that are brought onto site by staff and visitors are the responsibility of the user.
 - All members of Bantock Primary School community are advised to take steps to protect their mobile phones or personal 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 Bantock 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 in all areas with pupils within the site, particularly classrooms and 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 in line with our anti-bullying and behaviour policies.
- All members of Bantock 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.

9.2 Staff use of personal devices including mobile phones and smart watches.

- 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 of technology.
- Staff will be advised to
 - keep mobile phones and personal devices in a safe and secure place when pupils are in the area.
 - 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 such as in emergency circumstances.
 - ensure that any content brought onto site is only done so via provided equipment and 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.
 - Any pre-existing relationships which could undermine this, will be discussed with the DSL (or deputy) and headteacher.
- Staff will not use personal devices or mobile phones:

- to take photos or videos, **or share images** of learners and will only use work-provided equipment for this purpose.
- 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 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 using a personal device or mobile phone, the police will be contacted and the LADO (Local Authority Designated Officer) will be informed in line with our allegations policy.
- When accessing school data through a personal device, such as emails, device must have at least one of the following; 4+ digit pin code, finger print recognition or facial recognition to ensure that school data is secure if the device is lost or stolen.
- The use of removable media storage devices e.g. portable hard drives or memory sticks (USB flash drive) are not required for storing work as cloud storage (OneDrive) is available. It is not permitted to use these devices in order to minimize risks of data breaches.
- It is recommended that Bluetooth is turned off in the school building as they can allow routes to access data.
- **If staff members have a Smart Watch, these must be kept out of sight and not used around pupils at any time.**

9.3 Learners use of personal devices including mobile phones and smart watches

- 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.
- Bantock Primary School expects learners' personal devices and mobile phones to be handed in to the school office during school hours upon written permission between school and parents.
- If a learner needs to contact his/her parents or carers they will be allowed to use the school office phone.
 - Parents are advised to contact their child via the school office.
- Mobile phones or personal devices will not be used by learners during lessons or formal educational time.
- Mobile phones and personal devices must not be taken into examinations.
 - Learners 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 learner breaches the policy, the phone or device will be confiscated and held in a secure place.
 - Staff may confiscate a learner's mobile phone or device if they believe it is being used to contravene our child protection, behaviour or anti-bullying policy.
 - Searches of mobile phone or personal devices may be carried out in accordance with our policy in line with the DfE [Searching, Screening and Confiscation'](#) guidance.
 - 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 in line with the DfE [Searching, Screening and Confiscation'](#) guidance.
 - Mobile phones and devices that have been confiscated will be released to parents/ carers at the end of the day, following a discussion with the headteacher or DSL.

- 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.
- The use of imaging and image sharing technology, including, Smart Watches is prohibited due to privacy concerns, particularly with the ability to take photographs, as well as the risk of loss or theft, and distraction.

9.4 Visitors' use of personal devices and mobile phones

- Parents/carers and visitors, including volunteers and contractors, should ensure that mobile phones are not used in the presence of pupils.
- Appropriate information is provided to visitors upon entering the school.
- Visitors, including volunteers and contractors, who are on site for regular or extended periods of time are expected to use their mobile phones and personal devices in accordance with our acceptable use of technology policy and other associated policies, including but not limited to anti-bullying, behaviour, child protection and image use.
- Members of staff are expected to challenge visitors if they have concerns and inform the DSLs (or deputies) or headteacher of any breaches of our policy.

9.5 Officially provided mobile phones and devices

9.5.1 Staff Mobile

- Members of staff will be issued with a work phone for out of school visits, in case of emergency (see Visits and Visitors policy)
- The Bantock Primary School mobile phone is suitably protected via a pin and must only be accessed or used by members of staff.
- The Bantock Primary School mobile phone will always be used in accordance with the acceptable use of technology policy and other relevant policies.

9.5.2 Home Learning Devices

- Key Stage 2 pupils are offered a device to use for home learning, which is filtered and monitored.
- A parent must sign for responsibility of the device.
- Pupils are reminded of use in accordance with the Responsible and Acceptable Use Policy.
- Parents and pupils are reminded that these devices are only for accessing learning.
- Loaned devices are checked upon return to school to ensure that stored passwords are forgotten and browsing history is monitored and cleared before being loaned again.

10. Responding to Online Safety Incidents

- All members of the community will be made aware of the reporting procedure for online safety concerns, including breaches of filtering, peer on peer abuse, including cyberbullying and youth produced sexual imagery (sexting), online sexual violence and harassment, online abuse and exploitation and illegal content.
- All members of the community will 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 with us to resolve online safety issues.
- After any investigations are completed, leadership staff 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's (or deputies) will seek advice from the Multi Agency Safeguarding Hub (MASH)
- Where there is a concern that illegal activity has taken place, we will contact the police using 101, or 999 if there is immediate danger or risk of harm as appropriate.
- If information relating to a specific incident or a concern needs to be shared beyond our community, for example if other local settings are involved or the wider public may be at risk, the DSLs will speak with the police and the Education Safeguarding Service first, to ensure that potential criminal or child protection investigations are not compromised.
- **Refer to Appendix A's flowchart of strategies to respond to an Online Safety Concern**

10.1 Concerns about learner online behaviour and/or welfare

- The DSLs (or deputies) or DSM will be informed of all online safety concerns involving safeguarding or child protection risks in line with our Safeguarding and Child Protection policy.
- All concerns about learners will be recorded in line with our Safeguarding and Child Protection policy.
- Bantock Primary School recognises that whilst risks can be posed by unknown individuals or adults online, learners can also abuse their peers; all online peer on peer abuse concerns will be responded to in line with our child protection and behaviour policies.
- The DSLs (or deputies) or DSMs will ensure that online safety concerns are escalated and reported to relevant partner agencies in line with local policies and procedures.
- Appropriate sanctions and/or pastoral/welfare support will be offered to learners as appropriate. Civil or legal action will be taken if necessary.
- We will inform parents/carers of online safety incidents or concerns involving their child, as and when required.

10.2 Concerns about staff online behaviour and/or welfare

- Any complaint about staff misuse will be referred to the manager in accordance with our Whistleblowing Policy.
- Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- Appropriate disciplinary, civil and/or legal action will be taken in accordance with our staff Code of Conduct.
- Welfare support will be offered to staff as appropriate.

10.3 Concerns about parent/carer online behaviour and/or welfare

- Concerns regarding parents/carers behaviour and/or welfare online will be reported to the headteacher and/or DSLs (or deputies). They will respond to concerns in line with existing policies, including but not limited to child protection, anti-bullying, complaints, allegations against staff, home-school agreements, Responsible and Acceptable use of technology and behaviour policy.
- Civil or legal action will be taken if necessary.
- Welfare support will be offered to parents/carers as appropriate.

11. Procedures for Responding to Specific Online Concerns

11.1 Online sexual violence and sexual harassment between children

- The headteacher, DSL and appropriate members of staff have accessed and understood part 5 of ['Keeping children safe in education'](#)

- Full details of our response to peer on peer abuse, including sexual violence and harassment can be found in our Safeguarding and Child Protection Policy.
- Bantock 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
 - ‘Upskirting’, which typically involves taking a picture under a person’s clothing without them knowing, with the intention of obtaining sexual gratification, or causing the victim humiliation, distress or alarm. It is a criminal offence
 - Unwanted sexual comments and messages on social media
 - Online sexual exploitation
- 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 any concerns relating to online sexual violence and sexual harassment, we will:
 - immediately notify the DSLs (or deputies) and act in accordance with our child protection and anti-bullying policies.
 - if content is contained on learners personal devices, they will be managed in accordance with the DfE [‘searching screening and confiscation’](#) advice.
 - provide the necessary safeguards and support for all learners involved, such as implementing safety plans, offering advice on blocking, reporting and removing online content, and providing appropriate counselling/pastoral support.
 - implement appropriate sanctions in accordance with our behaviour policy.
 - inform parents and carers, if appropriate, about the incident and how it is being managed.
 - If appropriate, make referrals to partner agencies, such as Multi Agency Safeguarding Hub (MASH) and/or the police.
 - if the concern involves children and young people at a different educational setting, the DSL will 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 DSLs (or deputies) 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.
- Bantock Primary School 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.
- Bantock Primary School recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
- To help minimise concerns, Bantock 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 by implementing a range of age and ability appropriate educational methods as part of our curriculum.
- We will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between learners.

11.2 Youth produced sexual imagery (“sexting”)

- Bantock Primary School recognises youth produced sexual imagery (also 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 UKCIS guidance: [‘Sexting in schools and colleges: responding to incidents and safeguarding young people’](#)
 - Youth produced sexual imagery or ‘sexting’ is defined as the production and/or sharing of sexual photos and videos of and by young people who are under the age of 18. It includes nude or nearly nude images and/or sexual acts.
 - It is an offence to possess, distribute, show and make indecent images of children. The Sexual Offences Act 2003 defines a child, for the purposes of indecent images, as anyone under the age of 18.
- Bantock Primary School will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of creating or sharing youth produced sexual imagery by implementing preventative approaches, via a range of age and ability appropriate educational methods, such as through the JIGSAW and ProjectEVOLVE / ‘Education for a Connected World’ lessons.
- We will ensure that all members of the community are aware of sources of support regarding the taking and sharing of youth produced sexual imagery.
- We will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on site or using setting provided or personal equipment.
- We will not:
 - view any suspected youth produced sexual imagery, unless there is no other option, or there is a clear safeguarding need or reason to do so.
 - If it is deemed necessary, the imagery will only be viewed where possible by the DSLs, and any decision making will be clearly documented.
 - send, share, save or make copies of content suspected to be an indecent image/video of a child (i.e. youth produced sexual imagery) and will not allow or request learners 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 procedures.
 - ensure the DSLs (or deputies) respond in line with the [UKCIS](#) guidance.
 - Store any devices containing potential youth produced sexual imagery securely
 - If content is contained on learners personal devices, they will be managed in accordance with the DfE [‘searching screening and confiscation’](#) advice.
 - If a potentially 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 in line with the [UKCIS](#) guidance which considers the age and vulnerability of learners involved, including the possibility of carrying out relevant checks with other agencies.
 - inform parents/carers about the incident and how it is being managed and provide support and signposting, as appropriate.
 - make a referral to MASH and/or the police, as deemed appropriate in line with the [UKCIS](#) guidance.
 - provide the necessary safeguards and support for learners, such as offering counselling or pastoral support.
 - implement appropriate sanctions in accordance with our behaviour policy but taking care not to further traumatise victims where possible.
 - consider the deletion of images in accordance with the [UKCIS](#) 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 abuse and exploitation (including child sexual abuse and sexual or criminal exploitation)

- Bantock Primary School recognises online abuse and exploitation, including sexual abuse and sexual or criminal exploitation, as a safeguarding issue and all concerns will be reported to and dealt with by the DSL's (or deputies), in line with our safeguarding and child protection policy.
- Bantock Primary School will ensure that all members of the community are aware of online child abuse and sexual or criminal exploitation, including the possible grooming approaches which may be employed by offenders to target learners, and understand how to respond to concerns.
- We will implement preventative approaches for online child abuse and exploitation via a range of age and ability appropriate education for learners, staff and parents/carers.
- We will ensure that all members of the community are aware of the support available regarding online child abuse and exploitation, both locally and nationally.
- We will ensure that the 'Click CEOP' report button used to report online child sexual abuse is visible and available to learners and other members of our community. This can be found easily in multiple parts of the school website.
- If made aware of an incident involving online child abuse and/or exploitation, we will:
 - act in accordance with our child protection policies and the relevant KSCMP procedures.
 - store any devices containing evidence securely.
 - If content is contained on learners personal devices, they will be managed in accordance with the DfE '[searching screening and confiscation](#)' advice.
 - If any evidence is stored on our network or devices, we will act to block access to other users and isolate the content.
 - if appropriate, make a referral to MASH and inform the police via 101, or 999 if a learner is at immediate risk.
 - carry out a risk assessment which considers any vulnerabilities of learner(s) involved, including carrying out relevant checks with other agencies.
 - inform parents/carers about the incident and how it is being managed and provide support and signposting, as appropriate.
 - provide the necessary safeguards and support for learners, 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 abuse and exploitation, regardless of whether the incident took place on our premises or using setting provided or personal equipment.
 - Where possible and appropriate, learners will be involved in decision making. If appropriate, they will be empowered to report concerns themselves with support, for example if the concern relates to online sexual abuse via CEOP: www.ceop.police.uk/safety-centre/
- If we are unclear whether a criminal offence has been committed, the DSLs (or deputies) will obtain advice immediately through MASH and/or police.
- If made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the police by the DSLs (or deputies).

- If members of the public or learners at other settings are believed to have been targeted, the DSLs (or deputies) will seek advice from the police and/or the Education Safeguarding Service before sharing specific information to ensure that potential investigations are not compromised.

11.4 Indecent Images of Children (IIOC)

- Bantock Primary School will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC) as appropriate to the age and ability.
- 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 Internet Watch Foundation (IWF) block list and by implementing appropriate filtering, firewalls and anti-spam software.
- If we are unclear if a criminal offence has been committed, the DSLs (or deputies) will obtain advice immediately through the police and/or the Education Safeguarding Service.
- If made aware of IIOC, we will:
 - act in accordance with our child protection policy and the relevant KSCMP procedures.
 - store any devices involved securely.
 - immediately inform appropriate organisations, such as the IWF and police.
- If made aware that a member of staff or a learner has been inadvertently exposed to indecent images of children, we will:
 - ensure that the DSLs (or deputies) are informed.
 - ensure that the URLs (webpage addresses) which contain the suspect images are reported to the IWF 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 DSLs (or deputies) are informed.
 - ensure that the URLs (webpage addresses) which contain the suspect images are reported to the IWF via www.iwf.org.uk .
 - inform the police via 101 or 999 if there is an immediate risk of harm, and Children's Social Work Service, as appropriate.
 - only store copies of images (securely, where no one else has access to them and delete all other copies) following a written request from the police.
 - report concerns, as appropriate to parents/carers.
- If made aware that a member of staff is in possession of indecent images of children on a school provided devices, we will:
 - ensure that the headteacher is informed in line with our managing allegations against staff policy.
 - inform the Local 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 Online bullying

- Online bullying, along with all other forms of bullying, will not be tolerated at Bantock Primary School.

- Full details of how we will respond to online bullying are set out in our Anti-bullying Policy.

11.6 Online hate

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at Bantock Primary School and will be responded to in line with existing policies, including child protection, 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 DSLs (or deputies) will obtain advice through the Education Safeguarding Service and/or the police.

11.7 Online radicalisation and extremism

- As listed in this policy, we will take all reasonable precautions, including filtering, to ensure that learners and staff are safe from terrorist and extremist material when accessing the internet on site.
- If we are concerned that a learner or adult may be at risk of radicalisation online, the DSLs (or deputies) 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 headteacher will be informed immediately, and action will be taken in line with the safeguarding and child protection and managing allegations policies.

11.8 Harmful online challenges and online hoaxes

A hoax is a deliberate lie designed to seem truthful, and online challenges generally involve users recording themselves taking a challenge, and then distributing the video through social media channels, inspiring or daring others to repeat the challenge.

Staff at Bantock will be mindful that some children will struggle to identify harmful online challenges and online hoaxes.

What to do when a harmful online challenge or online hoax might be circulating between children

The school's Designated Safeguarding Leads (DSLs) and the Digital Safeguarding Manager (DSM) will be best placed to lead and provide any formal responses if deemed necessary.

The school will undertake case-by-case assessment, establishing the scale and nature of the possible risk to the children, including considering (where the evidence allows) if the risk is a national one or is it localised to the area, or even just this school.

The DSL's will check the factual basis of any harmful online challenge or online hoax with a known, reliable trustworthy source, such as the Professional Online Safety Helpline (<https://www.saferinternet.org.uk/professionals-online-safety-helpline>) from the UK Safer Internet Centre. Where harmful online challenges or online hoaxes appear to be local (rather than large scale national ones) local safeguarding advice, such as from the local authority or local police force, may also be appropriate and helpful.

Is it an online hoax?

The school will consider carefully if a challenge or scare story is a hoax. Generally speaking, naming an online hoax and providing direct warnings is not helpful. Concerns are often fuelled by unhelpful publicity, usually generated on social media, and may not be based on confirmed or factual occurrences or any real risk to children. There have been examples of hoaxes where much of the content was created

by those responding to the story being reported, needlessly increasing children's exposure to distressing content.

Is it a real online challenge that might cause harm to children?

If we are confident children are aware of, and engaged in, a real challenge that may be putting them at risk of harm, then it would be appropriate for this to be directly addressed. The school will carefully weigh up the benefits of school-wide highlighting of the potential harms related to a challenge against needlessly increasing children's exposure to it.

Exposing children to upsetting or scary content will be counterproductive and potentially harmful. If, as a school we do feel it is necessary to directly address an issue, this will be achieved without exposing children to scary or distressing content.

Whatever the school response, the following factors will be taken into account:

- Is it factual?
- Is it proportional to the actual (or perceived) risk?
- Is it helpful?
- Is it age and stage of development appropriate?
- Is it supportive?

When dealing with harmful online challenges and viral online hoaxes, there can be added pressure from parents and carers for school to directly address concerns. The DSL's will consider how best to manage these anxieties, and reassure concerned parents and carers, whilst not making the situation worse.

If a child raises concerns about a harmful online challenge or online hoax directly

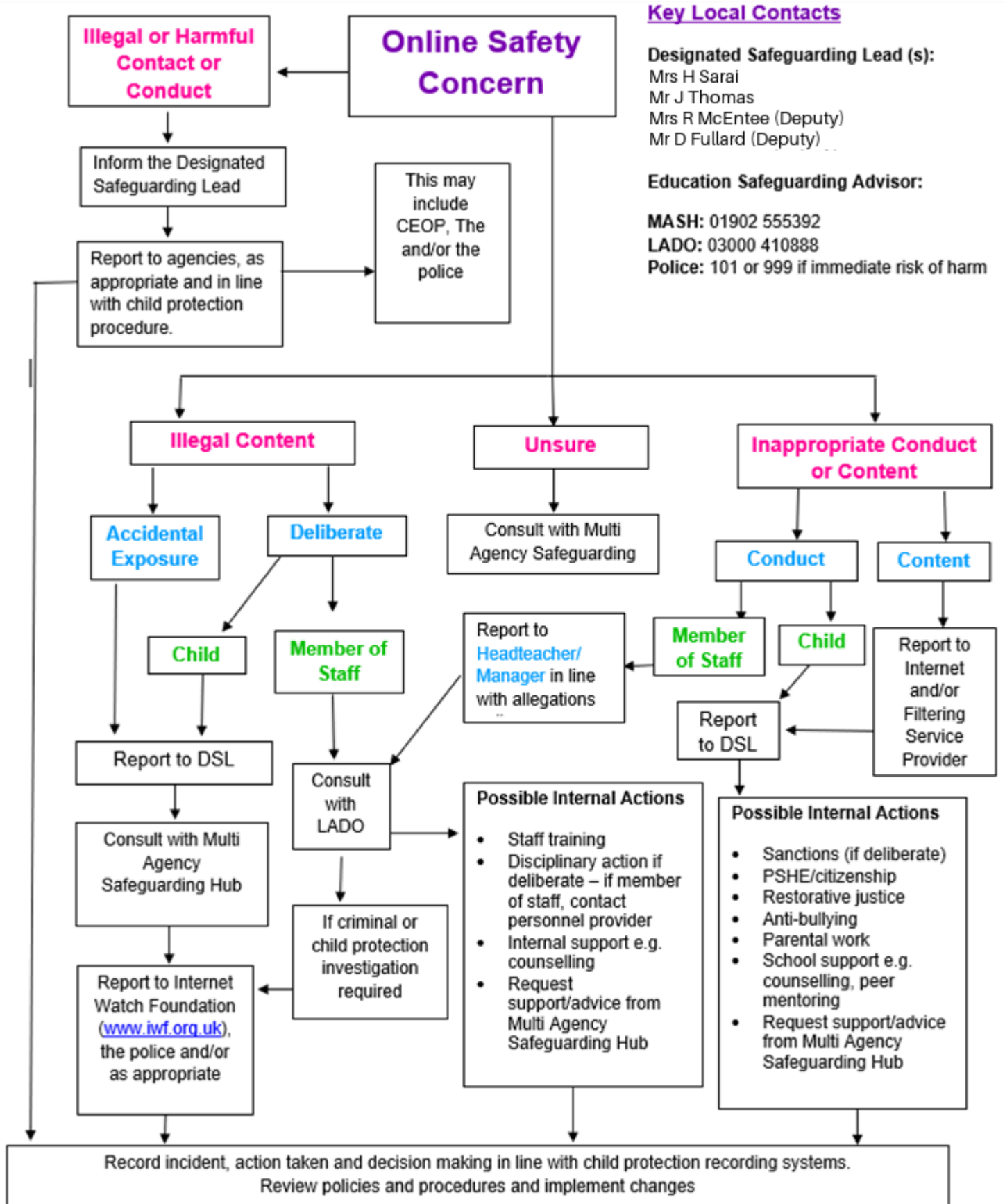
The school will consider the best way to speak to individual children, or where appropriate, in classes (but as already stated, be mindful of needlessly exposing all children to something they may not even be aware of or concerned about).

While acknowledging it, if it has been raised directly, we will avoid overly focusing on whatever the latest harmful online challenge or online hoax might be. The focus will be on what good online behaviour looks like, i.e. what to do if they see something upsetting online and who and where to report it.

Further Support

- The "digital ghost stories" report (<https://swgfl.org.uk/magazine/digital-ghost-stories/>) looks at the impact and risk of hoaxes
- UK Safer Internet Centre (<http://www.saferinternet.org.uk/>) provides advice for school on responding to online challenges
- Samaritans (<https://www.samaritans.org/>) shares information about challenges relating to suicide and self-harm research into online suicide challenges

Appendix A: Responding to an Online Safety Concern



Useful Links

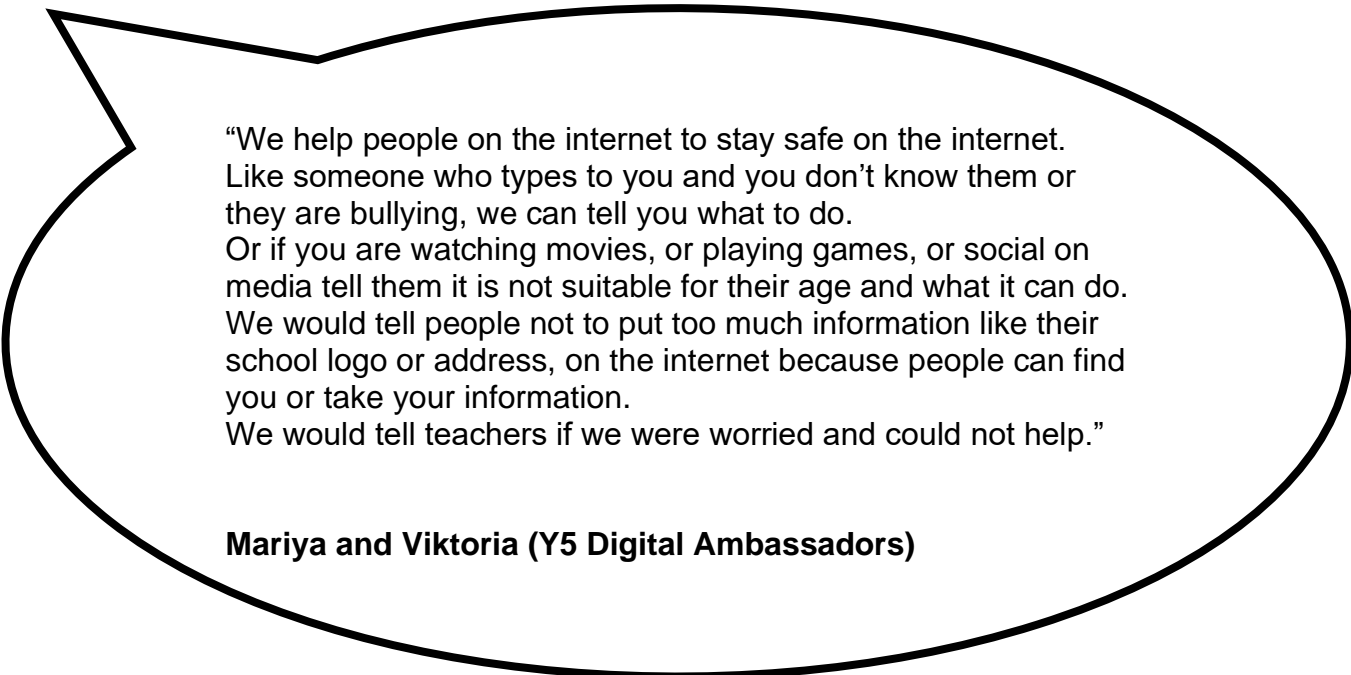
National Links and Resources for Settings, Learners and Parents/carers

- CEOP:
 - www.thinkuknow.co.uk
 - www.ceop.police.uk
- Internet Watch Foundation (IWF): www.iwf.org.uk
- UK Council for Internet Safety (UKCIS): www.gov.uk/government/organisations/uk-council-for-internet-safety
UK Safer Internet Centre: www.saferinternet.org.uk
 - Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
 - Report Harmful Content: <https://reportharmfulcontent.com/>
- 360 Safe Self-Review tool for schools: www.360safe.org.uk
- Childnet: www.childnet.com
 - Step Up Speak Up – Online Sexual Harassment Guidance: www.childnet.com/resources/step-up-speak-up/guidance-and-training-for-schools-and-professionals
 - Cyberbullying Guidance: www.childnet.com/resources/cyberbullying-guidance-for-schools
- Internet Matters: www.internetmatters.org
- Parent Zone: <https://parentzone.org.uk>
- Parent Info: <https://parentinfo.org>
- NSPCC: www.nspcc.org.uk/onlinesafety
 - ChildLine: www.childline.org.uk
 - Net Aware: www.net-aware.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- Action Fraud: www.actionfraud.police.uk
- Get Safe Online: www.getsafeonline.org
- NSPCC Learning - [Undertaking remote teaching safely during school closures](#)
- National Cyber Security Centre <https://www.ncsc.gov.uk/>

Acknowledgements and Thanks

- This document and statements have been developed from The Education People Education Safeguarding Service Policy alongside members of Kent Education Online Safety Strategy Group, as well as the South West Grid for Learning. Supported by Patrick Flynn of Online Behaviours.
- Additional thanks to the UK Safer Internet Centre, Childnet , CEOP, The Judd School, Kingsnorth Primary School, Loose Primary School, Peter Banbury, Kent Police, Kent Schools Personnel Service (SPS), Kent Legal Services and Kent Libraries and Archives, for providing comments, feedback and support on previous versions.

Digital Ambassadors



“We help people on the internet to stay safe on the internet. Like someone who types to you and you don’t know them or they are bullying, we can tell you what to do. Or if you are watching movies, or playing games, or social on media tell them it is not suitable for their age and what it can do. We would tell people not to put too much information like their school logo or address, on the internet because people can find you or take your information. We would tell teachers if we were worried and could not help.”

Mariya and Viktoria (Y5 Digital Ambassadors)

Digital 5 a Day

Connect

- Maintain friendships and family relationships
 - Know who you are talking to
 - Check your privacy settings

Be Active

- Exercise regularly
- Have screen breaks
- Research activities online

Get Creative

- Use coding or make video content to be creative and build digital skills
 - Be an active, not passive user of technology
- Use technology for education, using skills or learning new skills

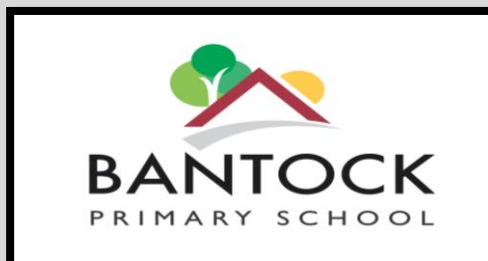
Give to Others

- Give positive feedback to others
- Report negative behaviour of others
- Use the internet to find out how to support local and national charities.
 - Make the web a positive place for everyone

Be Mindful

- Limit the time you use technology
- Don't give in to the pressure of technology and other people.
 - Understand how you and other people feel

You are responsible for making the right choices.



Appendix C Approved Technology Service Management

Name of Service	Location	School Admin	Sign In Method Password/Microsoft SSO/MFA	Data Processing Manual Input/Wonde/Automate
Arbor	Cloud	HT / Business Manager	Password	Manual Input
Microsoft	Cloud	HT / Business Manager	Teachers: MFA / Pupils: Password	Automate
Smart	App/Cloud		Microsoft SSO	Automate
Senso	Cloud	HT	Password	Automate
Century	Cloud	Technology Manager	Microsoft SSO	Automate
Education City	Cloud	Technology Manager	Password *	Wonde
FFT Aspire	Cloud	English Manager	Password	Wonde
Purple Mash	Cloud	Technology Manager	Password *	Wonde
TimesTable Rockstars	Cloud/App	Maths Manager	Password	Wonde
Class Dojo	Cloud		Password	
Flash Academy	Cloud/App		Password	
SPAG.com	Cloud		Password	
Evidence.Me	Cloud/App	Technology Manager	Password	Manual Input
Test Base			Password	
Grammarsaurus			Password	
Charanga	Cloud		Password	
Reception Baseline	Cloud	EY Manager	Password	Manual Input
Word Press (website)	Cloud	Technology Manager	Password	
Evolve	Cloud		Password	
Twinkl	Cloud	Business Manager	Password	Manual Input