BOURNE PRIMARY SCHOOL

Online Safety and Awareness Policy
(Including E-safety, Social Media and Acceptable Use for Pupils and Staff)

1. Creating an Online Safety Ethos

1.1 Aims and policy scope

- Bourne School believes that online safety (e-Safety) is an essential element of safeguarding children and adults in the digital world, when using technology such as computers, tablets, mobile phones or games consoles. It is deemed a child protection issue, as opposed to an ICT issue.
- Bourne School identifies that the internet and information communication technologies are an important part of everyday life, so children must be supported to be able to learn how to develop strategies to manage and respond to risk and be empowered to build resilience online.
- Bourne School has a duty to provide the school community with quality Internet access to raise education standards, promote pupil achievement, support professional work of staff and enhance the schools management functions.
- Bourne School identifies that there is a clear duty to ensure that children are protected from potential harm online.
- Online safety is not limited to school premises, school equipment or the school day. Online safety is a partnership concern (ie an incident occurring outside school and brought to the school's attention will be treated as if it had happened on school premises in the teaching day).
- Parents and staff need to understand that children often use computers in a different way to adults, especially at home. Whereas adults download, consume, access static corporate sites and use separate media, children tend to upload, create, access interactive personal sites and use converged media.
- It is increasingly common for children to use technology to post images and information about themselves and others; seek friendship; talk about others (sometimes in a hostile manner); use inappropriate (sometimes sexual) nicknames; express insecurities or fantasies; trick others or engage in dangerous acts using video or images; and generally push boundaries.
- Nationally, it is thought that parents underestimate the extent to which their own children:
    - view/engage in/are exposed to inappropriate material/language/behaviour;
    - disclose personal information;
    - engage in the inappropriate use of social networking sites; or
    - encounter incidents of grooming or cyber-bullying.
- Therefore, staff need to be vigilant, work in partnership with parents and other agencies and equip children with the skills they need to deal with these threats.

1.2 Purpose

The purpose of Bourne School online safety policy is to:

- Clearly identify the key principles expected of all members of the community with regards to the safe and responsible use technology to ensure that Bourne School is a safe and secure environment.
- Safeguard and protect all members of Bourne School community online.
- Raise awareness with all members of Bourne School community regarding the potential risks as well as benefits of technology.

- To enable all staff to work safely and responsibly, to role model positive behaviour online and be aware of the need to manage their own standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns that are known by all members of the community.
- The measures described are intended to protect children from:
    - exposure to inappropriate content;
    - exposure to strangers who, in the worst cases, may try to arrange to meet with children using email or chat rooms. (This is often referred to as 'grooming');
    - exposure to aggressive marketing and gambling or shopping sites which may encourage children to make unauthorised online transactions;
    - exposure to sites which embody values which parents and/or the school deem unhealthy or inappropriate;
    - child abuse;
    - cyber-bullying
    - exposure to possible radicalisation or extremist views as defined in the school's PREVENT policy and strategy

- This policy applies to all staff including the governing body, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for or provide services on behalf of the school (collectively referred to as 'staff' in this policy) as well as children and parents/carers.
- This policy applies to all access to the internet and use of information communication devices including personal devices or where children, staff or other individuals have been provided with school issued devices for use off-site, such as a work laptops, tablets or mobile phones.
- This policy must be read in conjunction with other relevant school policies.

1.3 Areas of Risk

The main areas of risk for our school community can be summarised as follows:

1.3.1 Content
- exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language and misogynist language and scenarios), substance abuse
- lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- hate sites
- exposure to websites connected to radicalisation and extremism
- content validation: how to check authenticity and accuracy of online content

1.3.2 Contact
- grooming
- grooming for radicalisation
- cyber-bullying in all forms
- identity theft (including 'frape' (hacking Facebook profiles) and sharing passwords

1.3.3 Conduct
- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being (amount of time spent online (internet or gaming)
- sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)

- copyright (little care or consideration for intellectual property and ownership – such as music and film)

1.4 Key responsibilities:

All members of school communities have an essential role to play in ensuring the safety and wellbeing of others, both on and offline. It is important that all members of the community are aware of these roles and responsibilities and also how to access and seek support and guidance:

1.4.1 Key responsibilities of the school management team:

- Developing, owning and promoting the online safety vision and culture to all stakeholders, in line with national and local recommendations with appropriate support and consultation throughout the school community.
- Ensuring that online safety is viewed by the whole community as a safeguarding issue and proactively developing a robust online safety culture.
- Supporting the DSL by ensuring they have sufficient time and resources to fulfil their online safety role and responsibilities.
- Auditing and evaluating current online safety practice to identify strengths and areas for improvement.
- Ensuring there are appropriate and up-to-date policies and procedures regarding online safety.
- To ensure that suitable and appropriate filtering and monitoring systems are in place to protect children from inappropriate content which meet the needs of the school community whilst ensuring children have access to required educational material.
- To work with and support technical staff in monitoring the safety and security of school systems and networks and to ensure that the school network system is actively monitored.
- Ensuring all members of staff receive regular, up-to-date and appropriate training regarding online safety roles and responsibilities and provide guidance regarding safe appropriate communications.
- Ensuring that online safety is embedded within a progressive whole school curriculum which enables all pupils to develop an age-appropriate understanding of online safety and the associated risks and safe behaviours.
- Making appropriate resources available to support the development of an online safety culture.
- Taking responsibility for online safety incidents and liaising with external agencies and support as appropriate.
- Receiving and regularly reviewing online safety incident logs and using them to inform and shape future practice.
- Ensuring there are robust reporting channels for the school community to access regarding online safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology, including ensuring the safe and responsible use of devices.
- To ensure a member of the Governing Body is identified with a lead responsibility for supporting online safety.
- To ensure that the DSL works in partnership with the online safety/e-Safety lead.

1.4.2 The key responsibilities of the Designated Safeguarding Lead are:

- Acting as a named point of contact on all online safeguarding issues and liaising with other members of staff and other agencies as appropriate.

- Keeping up-to-date with current research, legislation and trends regarding online safety.
- Coordinating participation in local and national events to promote positive online behaviour, e.g. Safer Internet Day.
- Ensuring that online safety is promoted to parents and carers and the wider community through a variety of channels and approaches.
- Work with the school lead for data protection and data security to ensure that practice is in line with current legislation.
- Maintaining a record of online safety concerns/incidents and actions taken as part of the schools safeguarding recording structures and mechanisms. Monitor the school s online safety incidents to identify gaps/trends and use this data to update the school s education response to reflect need
- To report to the school management team, Governing Body and other agencies as appropriate, on online safety concerns and local data/figures.
- Liaising with the local authority and other local and national bodies, as appropriate.
- Reviewing and updating online safety policies, Acceptable Use Policies (AUPs) and other related procedures on a regular basis (at least annually) with stakeholder input.
- Ensuring that online safety is integrated with other appropriate school policies and procedures.
- Leading an online safety team/group with input from all stakeholder groups.
- Meet regularly with the governor/board/committee member with a lead responsibility for online safety

1.4.3 Key responsibilities of staff

All members of staff play an essential role in creating a safe culture within settings, both on and offline. All members of staff should seek to promote safe and responsible online conduct with and by children as part of the curriculum and as part of their safeguarding responsibilities. All members of staff will need to role model positive behaviours when using technologies, either directly with children or in the wider context. All staff should be aware of and ensure they adhere to the school Acceptable Use Policies (AUPs).

The key responsibilities for all members of staff are:

- Contributing to the development of online safety policies.
- Reading the school Acceptable Use Policies (AUPs) and adhering to them.
- Taking responsibility for the security of school systems and data.
- Having an awareness of a range of online safety issues and how they relate to the children in their care.
- Modelling good practice when using new and emerging technologies
- Embedding online safety education in curriculum delivery wherever possible.
- Identifying individuals of concern and taking appropriate action by following school safeguarding policies and procedures.
- Knowing when and how to escalate online safety issues, internally and externally.
- Being able to signpost to appropriate support available for online safety issues, internally and externally.
- Maintaining a professional level of conduct in their personal use of technology, both on and off site.
- Demonstrating an emphasis on positive learning opportunities.
- Taking personal responsibility for professional development in this area.

1.4.4 In addition to the above, the key responsibilities for staff managing the technical environment are:

- Providing a safe and secure technical infrastructure which support safe online practices while ensuring that learning opportunities are still maximised.
- Taking responsibility for the implementation of safe security of systems and data in partnership with the leadership and management team.
- To ensure that suitable access controls and encryption is implemented to protect personal and sensitive information held on school-owned devices.
- Ensuring that the schools filtering policy is applied and updated on a regular basis and that responsibility for its implementation is shared with the DSL.
- Ensuring that the use of the school 's network is regularly monitored and reporting any deliberate or accidental misuse to the DSL.
- Report any breaches or concerns to the DSL and leadership team and together ensure that they are recorded and appropriate action is taken as advised.
- Developing an understanding of the relevant legislation as it relates to the security and safety of the technical infrastructure.
- Report any breaches and liaising with the local authority (or other local or national bodies) as appropriate on technical infrastructure issues.
- Providing technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Ensuring that the school's ICT infrastructure/system is secure and not open to misuse or malicious attack.
- Ensuring that appropriate anti-virus software and system updates are installed and maintained on all setting machines and portable devices.
- Ensure that appropriately strong passwords are applied and enforced for all but the youngest users.

1.4.5 The key responsibilities of children and young people are:

- Contributing to the development of online safety policies.
- Reading the school Acceptable Use Policies (AUPs) and adhering to them.
- Respecting the feelings and rights of others both on and offline.
- Seeking help from a trusted adult if things go wrong, and supporting others that may be experiencing online safety issues.
- At a level that is appropriate to their individual age, ability and vulnerabilities:
    - Taking responsibility for keeping themselves and others safe online.
    - Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
    - Assessing the personal risks of using any particular technology, and behaving safely and responsibly to limit those risks.

1.4.6. Key responsibilities of parents and carers

Parents /carers play a crucial role in developing children's safe and responsible online behaviours, especially where a majority of children's access will be taking place when they are not on the school site. Schools have a clear responsibility to work in partnership with families to raise awareness of online safety issues. Through this approach, parents/carers can help schools to reinforce online safety messages and promote and encourage safe online behaviours wherever, and whenever, children use technology.

The key responsibilities of parents and carers are:

- Reading the school Acceptable Use Policies, encouraging their children to adhere to them, and adhering to them themselves where appropriate.

- Discussing online safety issues with their children, supporting the school in their online safety approaches, and reinforcing appropriate safe online behaviours at home.
- Role modelling safe and appropriate uses of technology and social media.
- Identifying changes in behaviour that could indicate that their child is at risk of harm online.
- Seeking help and support from the school, or other appropriate agencies, if they or their child encounters online problems or concerns.
- Contributing to the development of the school online safety policies.
- Using school systems, such as learning platforms, and other network resources, safely and appropriately.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.

2. Online Communication and Safer Use of Technology

2.1 Schools and settings will be using a variety of online communication and collaboration tools both informally and formally with children, parents/carers and staff. It will be important that managers and leaders are aware of this use and provide clear boundaries and expectations for safe use.

2.2 The Technologies:
ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- The internet
- e-mail
- Instant messaging (e.g. Skype, messenger, Whatsapp, Kik) often using simple web cams
- Blogs (an on-line interactive diary)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Social networking sites (e.g. Facebook, Twitter, Instagram, SnapChat)
- Video broadcasting sites (e.g. youtube, musical.ly)
- Chat Rooms
- Gaming Sites
- Music download and streaming sites (e.g. iTunes, napster, spotify)
- Mobile phones with camera and video functionality
- Mobile technology (e.g. games consoles) that are 'internet ready'.
- Smart phones with e-mail, web functionality and cut down 'Office' applications.

2.3 Managing the school website

- The school will ensure that information posted on the school website meets the requirements as identified by the Department for Education.
- The contact details on the website will be the school address, email and telephone number. Staff or pupils' personal information will not be published.
- The head teacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.
- The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.
- Pupils work will be published with their permission or that of their parents/carers.
- The administrator account for the school website will be safeguarded with an appropriately strong password.

- The school will post information about safeguarding, including online safety, on the school website for members of the community.
- Photographs published on the web site do not have full names attached.
- Pupil's names are not used when saving images in the filenames or in the tags when publishing to the school website.

2.4 Publishing images and videos online

- The school will ensure that all images and videos shared online are used in accordance with the school image use policy.
- The school will ensure that all use of images and videos take place in accordance other policies and procedures including Codes of Conduct.
- In line with the image policy, written permission from parents or carers will always be obtained before images/videos of pupils are electronically published.
- The school will inform users about these risks and will implement policies to reduce the likelihood of the potential for harm:
  - When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images.
  - Particular focus should be given to recognising the risks attached to publishing their own images on the internet eg on social networking sites.
  - In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their own children at school events for their own personal use (as such use in not covered by the Data Protection Act), but **not** of other children.
  - To avoid photos being taken of other children, parents and carers are requested not to take photographs or videos during events, but to wait for a photo opportunity after the event
  - To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites.
  - Parents / carers should not comment on any activities involving other students / pupils in digital / video images.
  - Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images.
  - Digital / video images of on- or off-site school activities should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
  - Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
  - Pupils must not take, use, share, publish or distribute images of others without their permission
  - We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school
  - Permission from parents or carers will be obtained before photographs of students / pupils are published outside the school
  - Pupil's work can only be published outside of the school with the permission of the pupil and parents or carers.
  - Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils
  - Photographs will only be stored on password protected PCs by the Headteacher and website administrator.

2.5 Managing email

2.5.1 Students

- Pupils may only use school provided email accounts for educational purposes
- Children should be taught to report suspicious/unsolicited emails, especially those from parties not known to the school which encourage children to reply.
- Children are taught what to do if someone they don't know appears to be trying to contact them or communicates with them in an inappropriate way.
- Children to be instructed in responsible use of email and other messaging. They are taught to understand that they are not anonymous when using communications technology, and that their actions have consequences, just as they do in the real world.
- Children should be taught to recognise and report cyber-bullying.
- Children taught not to use email/messaging to arrange to meet or contact others without staff/parental authorisation.
- Personal use of e-mail by children is permitted at staff discretion and only when supervised.
- Emails should be checked by a member of staff before they are sent wherever possible.
- Email to be used out of school hours, for example by children in computer club, is under staff supervision only.
- No information which could lead to the unauthorised identification or contact of an individual child or adult by a member of the public may be emailed.
- Private contact details of children (other than the School's contact details) must not emailed.
- Whole -class or group email addresses may be used for communication outside of the school.

2.5.2 Staff

- All members of staff are provided with a specific email address to use for any official communication and should not be used for personal emails.
- The use of personal email addresses by staff for any official school business is not permitted.
- The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains any content which could be subject to data protection legislation (e.g. sensitive or personal information) will only be sent using secure and encrypted email.
- Members of the community must immediately tell a designated member of staff if they receive offensive communication and this will be recorded in the school safeguarding files/records. The school will contact the police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Knows that spam, phishing and virus attachments can make e-mails dangerous. We use a number of technologies to help protect users and systems in the school, including desktop anti-virus product Sophos, plus direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language.
- Excessive social email use can interfere with teaching and learning and will be restricted. Access in school to external personal email accounts may be blocked.
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be.

- School email addresses and other official contact details will not be used for setting up personal social media accounts.

2.6 Official videoconferencing and webcam use for educational purposes:

- The school acknowledges that videoconferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity.
- All videoconferencing equipment will be switched off when not in use and where appropriate, not set to auto answer.
- External IP addresses will not be made available to other sites.
- Videoconferencing contact details will not be posted publically.
- Staff will ensure that external videoconference opportunities and/or tools are suitably risk assessed and will ensure that accounts and systems used to access events are appropriately safe and secure.

2.6.1 Users

- Pupils will ask permission from a teacher before making or answering a videoconference call or message.
- Videoconferencing will be supervised appropriately for the pupils' age and ability.
- Parents and carers consent will be obtained prior to children taking part in videoconferencing activities.
- Video conferencing will take place via official and approved communication channels following a robust risk assessment.
- Only key administrators will be given access to videoconferencing administration areas or remote control pages.
- Unique log on and password details for the educational videoconferencing services will only be issued to members of staff and kept secure.

2.6.2 Content

- When recording a videoconference lesson, written permission will be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference. Recorded material will be stored securely.
- If third party materials are to be included, the school will check that recording is acceptable to avoid infringing the third party intellectual property rights.
- The school will establish dialogue with other conference participants before taking part in a videoconference. If it is a non-school site the school will check that they are delivering material that is appropriate for the class.

2.7 Appropriate and safe classroom use of the internet (and associated devices)

- Internet use is a key feature of educational access and all children will receive age and ability appropriate education to support and enable them to develop strategies to respond to concerns as part of an embedded whole school curriculum. Please access curriculum policies for further information.
- The school's internet access will be designed to enhance and extend education.
- Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.
- All members of staff are aware that they cannot rely on filtering alone to safeguard children and supervision, classroom management and education about safe and responsible use is essential.
- Supervision of pupils will be appropriate to their age and ability.
    - At Early Years Foundation Stage and Key Stage 1 pupils' 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 pupils' age and ability.
    - At Key Stage 2 pupils will be supervised. Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary. Children will be directed to online material and resources which support the learning outcomes planned for the pupils' age and ability.
- All school owned devices will be used in accordance with this policy with appropriate safety and security measure in place.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- The school will use age appropriate search tools as decided by the school following an informed risk assessment to identify which tool best suits the needs of our community.
- The school will ensure that the use of Internet-derived materials by staff and pupils complies with copyright law and acknowledge the source of information.
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.
- The school will use the internet to enable pupils and staff to communicate and collaborate in a safe and secure environment.

2.8 Management of school learning platforms/portals/gateways

- Leaders/managers and staff will regularly monitor the usage of the Learning Platform (LP) in all areas, in particular message and communication tools and publishing facilities.
- Pupils/staff will be advised about acceptable conduct and use when using the LP.
- Only members of the current pupil, parent/carers and staff community will have access to the LP.
- All users will be mindful of copyright issues and will only upload appropriate content onto the LP.
- When staff, pupils' etc. leave the school their account or rights to specific school areas will be disabled.
- 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.
    - The material will be removed by the site administrator if the user does not comply.
    - Access to the LP for the user may be suspended.
    - The user will need to discuss the issues with a member of leadership before reinstatement.
    - A pupil's parent/carer may be informed.
- A visitor may be invited onto the LP by a member of the leadership. In this instance there may be an agreed focus or a limited time slot.
- Pupils may require editorial approval from a member of staff. This may be given to the pupil to fulfil a specific aim and may have a limited time frame.

3. Social Media Policy

3.1. General social media use

- Expectations regarding safe and responsible use of social media will apply to all members of Bourne School community and exist in order to safeguard both the school and the wider community, on and offline. Examples of social media may include blogs,

wikis, social networking, forums, bulletin boards, multiplayer online gaming, apps, video/photo sharing sites, chatrooms, instant messenger and many others.

- All members of Bourne School community will be encouraged to engage in social media in a positive, safe and responsible manner at all times.
- Information about safe and responsible use of social media will be communicated clearly and regularly to all members of Bourne School community.
- All members of Bourne School community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
- The school will not permit pupil or staff access to social media and social networking sites whilst on site and using school provided devices and systems.
- The use of social networking applications during school hours for personal use is not permitted.
- Inappropriate or excessive use of social media during school/work hours or whilst using school devices may result in disciplinary or legal action and/or removal of Internet facilities.
- Any concerns regarding the online conduct of any member of Bourne School community on social media sites should be reported to the leadership team and will be managed in accordance with policies such as anti-bullying, allegations against staff, behaviour and safeguarding/child protection.
- Any breaches of school policy may result in criminal, disciplinary or civil action being taken and this will depend upon the age of those involved and the circumstances of the wrong committed. Action taken will be accordance with relevant policies, such as anti-bullying, behaviour, safeguarding and child protection including the allegations against staff section.

3.2 Official use of social media:

- Bourne School official social media channels are:
    - ***Bourne School Facebook page, Reception Facebook page***
- Official use of social media sites by the school will only take place with clear educational or community engagement objectives with specific intended outcomes e.g. increasing parental engagement.
- Official use of social media sites as communication tools will be risk assessed and formally approved by the Head Teacher.
- Official school social media channels will be set up as distinct and dedicated social media site or account for educational or engagement purposes.
- Staff will use school provided email addresses to register for and manage any official approved social media channels.
- Members of staff running official social media channels will sign a specific Acceptable Use Policy (AUP) to ensure they are aware of the required behaviours and expectations of use and to ensure that sites are used safely, responsibly and in accordance with local and national guidance and legislation.
- All communication on official social media platforms will be clear, transparent and open to scrutiny.
- Any online publication on official social media sites will comply with legal requirements including the Data Protection Act 1998, right to privacy conferred by the Human Rights Act 1998, or similar duty to protect private information and will not breach any common law duty of confidentiality, copyright etc.
- Official social media use will be in line with existing policies including anti-bullying and child protection and safeguarding.
- Images or videos of children will only be shared on official social media sites/channels in accordance with the image use policy.
- Information about safe and responsible use of social media channels will be communicated clearly and regularly to all members of the community.

- Official social media sites, blogs or wikis will be suitably protected (e.g. password protected) and where possible/appropriate, run and/or linked to from the school website and take place with written approval from the Leadership Team.
- Leadership staff must be aware of account information and relevant details for social media channels.
- Parents/Carers and pupils will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.
- Public communications on behalf of the school will, where possible, be read and agreed by at least one other colleague.
- Official social media channels will link back to the school website to demonstrate that the account is official.
- The school 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.

3.3 Staff personal use of social media:

- Personal use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the school Acceptable Use Policy.
- All members of staff are advised not to communicate with or add as 'friends' any current or past children/pupils or current or past pupils' family members via any personal social media sites, applications or profiles. Any pre-existing relationships or exceptions that may compromise this will be discussed with Designated Safeguarding Lead and/or a member of the Leadership Team/Headteacher.
- If ongoing contact with pupils is required once they have left the school roll, then members of staff will be expected to use existing alumni networks or use official school provided communication tools.
- All communication between staff and members of the school community on school business will take place via official approved communication channels such as an official setting provided email address or phone numbers.
- Staff will not use personal accounts or information to make contact with pupils or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the Head Teacher.
- Any communication from pupils/parents received on personal social media accounts will be reported to the designated safeguarding lead.
- Information staff members have access to as part of their employment, including photos and personal information about pupils and their family members, colleagues etc. will not be shared or discussed on personal social media sites.
- All members of staff are strongly advised to safeguard themselves and their privacy when using social media sites. This will include being aware of location sharing services, setting the privacy levels of their personal sites as strictly as they can, opting out of public listings on social networking sites, logging out of accounts after use and keeping passwords safe and confidential.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance with schools policies and the wider professional and legal framework.
- Members of staff will be encouraged to manage and control the content they share and post online. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis.
- Members of staff will notify the Leadership/Management Team immediately if they consider that any content shared or posted via any information and communications

technology, including emails or social networking sites conflicts with their role in the school.

- Members of staff are encouraged not to identify themselves as employees of Bourne School on their personal social networking accounts. This is to prevent information on these sites from being linked with the school and also to safeguard the privacy of staff members and the wider community.
- Member of staff will ensure that they do not represent their personal views as that of the school on social media.
- School email addresses will not be used for setting up personal social media accounts.
- Members of staff who follow/like the school social media channels will be advised to use dedicated professionals accounts, where possible, to avoid blurring professional boundaries.

3.4 Staff official use of social media:

- If members of staff are participating in online activity as part of their capacity as an employee of the school, then they are requested to be professional at all times and that they are an ambassador for the school.
- Staff using social media officially will disclose their official role/position but always make it clear that they do not necessarily speak on behalf of the school.
- Staff using social media officially will be responsible, credible, fair and honest at all times and consider how the information being published could be perceived or shared.
- Staff using social media officially will always act within the legal frameworks they would adhere to within the workplace, including libel, defamation, confidentiality, copyright, data protection as well as equalities laws.
- Staff must ensure that any image posted on any official social media channel have appropriate written parental consent.
- Staff using social media officially will be accountable and must not disclose information, make commitments or engage in activities on behalf of the school unless they are authorised to do so.
- Staff using social media officially will inform their line manager, the Designated Safeguarding Lead and/or the head teacher of any concerns such as criticism or inappropriate content posted online.
- Staff will not engage with any direct or private messaging with children or parents/carers through social media and will communicate via official communication channels.

3.5 Pupils' use of social media

- Safe and responsible use of social media sites will be outlined for children and their parents as part of the Online Safety Policy.
- Pupils will be advised to consider the risks of sharing personal details of any kind on social media sites which may identify them and/or their location. Examples would include real/full name, address, mobile or landline phone numbers, school attended, Instant messenger contact details, email addresses, full names of friends/family, specific interests and clubs etc.
- Pupils will be advised not to meet any online friends without a parent/carer or other responsible adult's permission and only when they can be present.
- Pupils will be advised on appropriate security on social media sites and will be encouraged to use safe and passwords, deny access to unknown individuals and be supported in learning how to block and report unwanted communications.
- Pupils will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private/protected.
- Parents will be informed of any official social media use with pupils and written parental consent will be obtained, as required.

- Any official social media activity involving pupils will be moderated by the school where possible.
- The school is aware that many popular social media sites state that they are not for children under the age of 13, therefore the school will not create accounts within school specifically for children under this age.
- Any concerns regarding pupils' use of social networking, social media and personal publishing sites, both at home and at school, will be dealt with in accordance with existing school policies including anti-bullying and behaviour.
- Any concerns regarding pupils' use of social networking, social media and personal publishing sites, both at home and at school, will be raised with parents/carers, particularly when concerning any underage use of social media sites.
- If personal information about a child is found on an unsecured or otherwise inappropriate site, individual parents will be notified, made aware of the risks and advised as to the steps which could be taken to prevent this breach of e-safety. The school may also seek permission from the parents to help the child make their site secure if the parents are unwilling to close the site down.

4. Use of Personal Devices and Mobile Phones

4.1 Rationale regarding personal devices and mobile phones

- The widespread ownership of mobile phones and a range of other personal devices among children, young people and adults will require all members of the Bourne School community to take steps to ensure that mobile phones and personal devices are used responsibly.
- Bourne School recognises that personal communication through mobile technologies is an accepted part of everyday life for children, staff and parents/carers but requires that such technologies need to be used safely and appropriately within schools/settings.
- The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom.

4.2 Expectations for safe use of personal devices and mobile phones

- All use of personal devices and mobile phones will take place in accordance with the law and other appropriate school policies -Staff Handbook and Code of Conduct.
- Electronic devices of all kinds that are brought in on site are the responsibility of the user at all times. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.
- Mobile phones and personal devices are not permitted to be used in certain areas within the school site such as toilets.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community and any breaches will be dealt with as part of the discipline/behaviour policy.
- Members of staff will be issued with a school email address where contact with pupils or parents/carers is required.
- All members of Bourne School community will be advised to take steps to protect their mobile phones or devices from loss, theft or damage.
- All members of Bourne School community will be advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices if they are lost or stolen. Passwords and pin numbers should be kept confidential. Mobile phones and personal devices should not be shared.
- All members of Bourne School community will be advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene the school's policies.

- School devices must always be used in accordance with the Acceptable Use Policy
- School mobile phones and devices used for communication with parents and pupils must be suitably protected via a passcode/password/pin and must only be accessed and used by members of staff.

4.3 Pupils use of personal devices and mobile phones

- Pupils will be educated regarding the safe and appropriate use of personal devices and mobile phones.
- All use of mobile phones and personal devices by children will take place in accordance with the acceptable use policy.
- Pupil's personal mobile phones and personal devices will be kept in a secure place, switched off and kept out of sight in the school office.
- If a pupil needs to contact his/her parents/carers they will be allowed to use a school phone.
- Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office. Exceptions may be permitted in exceptional circumstances on a case-by-case basis and as approved by the Head Teacher.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members.
- Pupils will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.
- Mobile phones and personal devices must not be taken into examinations. Pupils found in possession of a mobile phone or personal device during an exam will be reported to the appropriate examining body. This may result in the pupil's withdrawal from either that examination or all examinations.
- If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents/carers in accordance with the school policy.
- School staff may confiscate a pupil's mobile phone or device if they believe it is being used to contravene the schools behaviour or bullying policy. The phone or device may be searched by a member of the Leadership team with the consent of the pupil or parent/carer. Searches of mobile phone or personal devices will be carried out in accordance with the schools policy. (**See** (gov.uk) Searching Screening and Confiscation. If there is suspicion that material on a pupil's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence then the device will be handed over to the police for further investigation.

4.4 Staff use of personal devices and mobile phones:

Safer Practices: Bring Your Own Device (BYOD)

- At Bourne staff must not bring in their own ipads or laptops for use in school.
- Mobile phones brought into school are entirely at the staff member, students' & parents' or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- Members of staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity. Any pre-existing relationships which could compromise this will be discussed with leaders/managers.
- Staff will not use personal devices such as mobile phones, tablets or cameras to take photos or videos of children and will only use work-provided equipment for this purpose.
- Staff will not use any personal devices directly with children and will only use work-provided equipment during lessons/educational activities.

- Members of staff will ensure that any use of personal phones and devices will always take place in accordance with the law e.g. data protection as well as relevant school policy and procedures.
- Staff personal mobile phones and devices will be switched off/switched to 'silent' mode during lesson times.
- Bluetooth or other forms of communication should be "hidden" or switched off during lesson times.
- Personal mobile phones or devices will not be used during teaching periods unless permission has been given by a member of the Leadership Team in emergency circumstances.
- Staff will ensure that any content bought on site via mobile phones and personal devices are compatible with their professional role and expectations.
- If a member of staff breaches the school policy then disciplinary action will be taken.
- 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 then the police will be contacted.
- Any allegations against members of staff involving personal use of mobile phone or devices will be responded to following the school allegations management section in the safeguarding and child protection policy.

4.5 Visitors' use of personal devices and mobile phones

- Parents/carers and visitors must use mobile phones and personal devices in accordance with the school s acceptable use policy.
- Use of mobile phones or personal devices by visitors and parents/carers to take photos or videos is prohibited.
- The school will ensure appropriate signage and information is displayed and provided to inform visitors of expectations of use.
- Staff will be expected to challenge concerns when safe and appropriate and will always inform the Designated Safeguarding Lead of any breaches of use by visitors.

5. Policy Decisions

5.1. Reducing online risks

- Bourne School is aware that the Internet is a constantly changing environment with new apps, tools, devices, sites and material emerging at a rapid pace.
- Emerging technologies will be examined for educational benefit and the school leadership team will ensure that appropriate risk assessments are carried out before use in school is allowed.
- The school will ensure that appropriate filtering systems are in place to prevent staff and pupils from accessing unsuitable or illegal content. (Bourne School uses Smoothwall Web Filtering provided by Schools ICT Services.
- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not always possible to guarantee that access to unsuitable material will never occur via a school computer or device.
- The school will audit technology use to establish if the online safety (e–Safety) policy is adequate and that the implementation of the policy is appropriate.
- Methods to identify, assess and minimise online risks will be reviewed regularly by the school leadership team.

5.2. Internet use throughout the wider school community

- The school will work with the local community's needs (including recognising cultural backgrounds, languages, religions and ethnicity) to ensure internet use is appropriate.

- The school will provide an Acceptable Use Policy for any guest/visitor who needs to access the school computer system or internet on site.

5.3 Authorising internet access

- The school will maintain a current record of all staff and pupils who are granted access to the school's devices and systems.
- All staff, pupils and visitors will read and sign the Acceptable Use Policy before using any school resources.
- Parents will be informed that pupils will be provided with supervised internet access which is appropriate to their age and ability.
- Parents will be asked to read the Acceptable Use Policy for pupil access and discuss it with their child, where appropriate.
- When considering access for vulnerable members of the community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the pupil(s).

6. Engagement Approaches

6.1 Engagement and education of children and young people:

Useful online safety (e-Safety) programmes include:

- Think U Know: www.thinkuknow.co.uk
- Childnet: www.childnet.com
- Kidsmart: www.kidsmart.org.uk
- Digital Literacy Scheme of Work: www.digital-literacy.org.uk
- Internet Matters: www.internetmatters.org
- BBC
    - www.bbc.co.uk/webwise
    - www.bbc.co.uk/cbbc/topics/stay-safe
    - www.bbc.co.uk/education

- An online safety (e-Safety) curriculum will be established and embedded throughout the whole school, to raise awareness regarding the importance of safe and responsible internet use amongst pupils.
- Education about safe and responsible use will precede internet access.
- All users will be informed that network and internet use will be monitored.
- Online safety (e-Safety) will be included in the PSHE, SRE, Citizenship and Computing programmes of study covering both safe school and home use.
- Online safety (e-Safety) education and training will be included as part of the transition programme across the Key Stages and when moving between establishments.
- Acceptable Use expectations and posters will be posted in all rooms with Internet access.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and within all subject areas.
- External support will be used to complement and support the schools internal online safety (e-Safety) education approaches.
- The school will reward positive use of technology by pupils.
- The school will implement peer education to develop online safety as appropriate to the needs of the pupils.

6.2 Engagement and education of children and young people who are considered to be vulnerable

- Bourne School is aware that some children may be considered to be more vulnerable online due to a range of factors.
- Bourne School will ensure that differentiated and ability appropriate online safety (e-Safety) education is given, with input from specialist staff as appropriate (e.g. SENCO).

6.3 Engagement and education of staff

- The online safety (e-Safety) policy will be formally provided to and discussed with all members of staff as part of induction and will be reinforced and highlighted as part of our safeguarding responsibilities.
- Staff will be made aware that our Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential when using school systems and devices.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff on a regular (at least annual) basis.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- Members of staff with a responsibility for managing filtering systems or monitor ICT use will be supervised by the Leadership Team and will have clear procedures for reporting issues or concerns.
- The school will highlight useful online tools which staff should use according to the age and ability of the pupils.

6.4 Engagement and education of parents and carers

- Bourne School recognises that parents/carers have an essential role to play in enabling children to become safe and responsible users of the internet and digital technology.
- Parents' attention will be drawn to the school online safety (e-Safety) policy and expectations in newsletters, letters, the school prospectus and on the school website.
- A partnership approach to online safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use or highlighting online safety at other well attended events e.g. parent evenings, transition events, fetes and sports days.
- Parents will be requested to read online safety information as part of the Home School Agreement.
- Parents will be encouraged to read the school Online Safety for pupils and discuss its implications with their children.
- Information and guidance for parents on online safety will be made available to parents in a variety of formats.
- Parents will be encouraged to role model positive behaviour for their children online.

7. Managing Information Systems

7.1 Managing personal data online

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

7.2 Security and Management of Information Systems

- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.

- Personal data sent over the Internet or taken off site (such as via portable media storage) will be encrypted or accessed via appropriate secure remote access systems.
- Portable media may not be used without specific permission followed by an anti-virus /malware scan.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the school's network will be regularly checked.
- The computing coordinator/network manager will review system capacity regularly.
- The appropriate use of user logins and passwords to access the school network will be enforced for all but the youngest users.
- All users will be expected to log off or lock their screens/devices if systems are unattended.
- The school will log and record internet use on all school owned devices, using the Smoothwall filtering console to display sites that were intervened.

7.3 Password policy

- All users will be informed not to share passwords or information with others and not to login as another user at any time.
- Staff and pupils must always keep their password private and must not share it with others or leave it where others can find it.
- All members of staff will have their own unique username and private passwords to access school systems. Members of staff are responsible for keeping their password private.
- We require staff and pupils to use STRONG passwords for access into our system.

7.4 Filtering Decisions

- The Leadership Team will ensure that the school has age and ability appropriate filtering and monitoring in place whilst using school devices and systems to limit children's exposure to online risks.
- The school's internet access strategy will be dependent on the need and requirements of our community and will therefore be designed to suit the age and curriculum requirements of our pupils, with advice from technical, educational and safeguarding staff.
- All monitoring of school owned/provided systems will take place to safeguard members of the community.
- All users will be informed that use of school systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.
- The school uses educational filtered secure broadband connectivity through the East Sussex Education Network which is appropriate to the age and requirement of our pupils.
- The school uses Smoothwall filtering systems which block sites that fall into categories such as pornography, racial hatred, extremism, sites of an illegal nature, etc.
- The school will work with Schools ICT to ensure that filtering policy is continually reviewed
- The school will have a clear procedure for reporting breaches of filtering which all members of the school community (all staff and all pupils) will be made aware of.
- If staff or pupils discover unsuitable sites, the URL will be reported to the School Designated Safeguarding Lead and will then be recorded and escalated as appropriate.
- The school filtering system will block all sites on the Internet Watch Foundation (IWF) list.
- Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Leadership Team.
- All changes to the school filtering policy will be logged and recorded.

- The Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective and appropriate.
- Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, East Sussex Police or CEOP immediately.

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

In recent years, a number of applications (apps) for mobile devices have been launched which are targeted specifically at education settings which allow staff to track and share a child's learning journey online with parents and carers, usually in the form of photographs and text. Such tools will have considerable benefits for setting and their communities, including improved engagement with parents and a reduction in paperwork, but careful consideration must be given to safeguarding and data security principles before using such tools.

- The school uses Tapestry to record and share EYFS learning journeys.
- The Head Teacher is ultimately responsible for the security of any data or images held of children.
- Apps/systems which store personal data will be risk assessed prior to use.
- Only school issued devices will be used for apps that record and store children's personal details, attainment or photographs. Personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store children's personal details, attainment or images.
- Users will be advised on safety measures to protect all members of the community such as using strong passwords, logging out of systems etc.
- Parents will be informed of the schools expectations regarding safe and appropriate use (e.g. not sharing passwords or sharing images) prior to being given access.

8. Responding to Online Incidents and Concerns

8.1 All members of the community will be made aware of the range of online risks that are likely to be encountered including sexting, online/cyber bullying etc. This will be highlighted within staff training and educational approaches for pupils.

8.2 All members of the school community will be informed about the procedure for reporting online safety (e-Safety) concerns, such as breaches of filtering, cyberbullying, illegal content etc.

8.3 The Designated Safeguarding Lead (DSL) will be informed of any online safety (e-Safety) incidents involving child protection concerns, which will then be recorded.

8.4 The DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Local Safeguarding Children Board thresholds and procedures.

8.5 Complaints

8.5.1 Complaints about Internet misuse will be dealt with under the School's complaints procedure.

8.5.2 Complaints about online bullying will be dealt with under the School's anti-bullying policy and procedure.

8.5.3 Any complaint about staff misuse will be referred to the head teacher.

8.5.4 Pupils, parents and staff will be informed of the school's complaints procedure.

8.6 Any allegations against a member of staff's online conduct will be discussed with the Local Authority Designated Officer (LADO).

8.7 Staff will be informed of the whistleblowing procedure.

8.8 All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.

8.9 All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.

8.10 The school will manage online safety (e-Safety) incidents in accordance with the school discipline/behaviour policy where appropriate.

8.11 The school will inform parents/carers of any incidents of concerns as and when required.

8.12 After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes as required.

8.13 Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the SLES Safeguarding Team or East Sussex Police via 101 or 999 if there is immediate danger or risk of harm.

8.14 The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to East Sussex Police.

8.15 If the school is unsure how to proceed with any incidents of concern, then the incident will be escalated to the SLES Safeguarding Team.

8.16 If an incident of concern needs to be passed beyond the school then the concern will be escalated to the SLES Safeguarding Team to communicate to other schools/settings in East Sussex.

8.17 Parents and children will need to work in partnership with the school to resolve issues.

9 Procedures for Responding to Specific Online Incidents or Concerns

9.1 Responding to concerns regarding Youth Produced Sexual Imagery or "Sexting"

Youth Produced Sexual Imagery or "Sexting" can be defined as images or videos generated by children under the age of 18 that are of a sexual nature or are considered to be indecent. These images may be shared between children and young people and/or adults via a mobile phone, webcam, handheld device or website.

- Bourne School ensures that all members of the community are made aware of the potential social, psychological and criminal consequences of sharing, possessing and creating youth produced sexual imagery (known as "sexting").
- The school will implement preventative approaches via a range of age and ability appropriate educational approaches for pupils, staff and parents/carers.
- Bourne School views "sexting" as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Lead (Claire Munro).
- The school will follow the guidance as set out in the non-statutory UKCCIS advice 'Sexting in schools and colleges: responding to incidents and safeguarding young people'.
- If the school are made aware of incident involving indecent images of a child the school will:

    - Act in accordance with the school's child protection and safeguarding policy and the relevant East Sussex Local Safeguarding Children Boards procedures.
    - Immediately notify the designated safeguarding lead.
    - Store the device securely.
    - Carry out a risk assessment in relation to the children(s) involved.
    - Consider the vulnerabilities of children(s) involved (including carrying out relevant checks with other agencies)
    - Make a referral to children's social care and/or the police (as needed/appropriate).
    - Put the necessary safeguards in place for children e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.
    - Inform parents/carers about the incident and how it is being managed.
    - Implement appropriate sanctions in accordance with the school's behaviour policy but taking care not to further traumatise victims where possible.
    - Review the handling of any incidents to ensure that the school is implementing best practice and the leadership team will review and update any management procedures where necessary.
- The school will not view an image suspected of being youth produced sexual imagery unless there is no other possible option or there is a clear need or reason to do so (in these cases the image will only be viewed by the Designated Safeguarding Lead).
- The school will not send, share or save indecent images of children and will not allow or request children to do so.
- If an indecent image has been taken or shared on the school's network or devices then the school will take action to block access to all users and isolate the image.
- The school will need to involve or consult the police if images are considered to be illegal.
- The school will take action regarding indecent images, regardless of the use of school equipment or personal equipment, both on and off the premises.
- The school will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.

9.2. Responding to concerns regarding Online Child Sexual Abuse and Exploitation

Online child sexual abuse within this policy context is specifically defined as when children are sexually abused or exploited via the use of technology and the internet. Typically this is referred to as "online grooming".

- Bourne School will ensure that all members of the community are made aware of online child sexual abuse, including exploitation and grooming including the consequences, possible approaches which may be employed by offenders to target children and how to respond to concerns.
- The school will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate educational approaches for pupils, staff and parents/carers.
- Bourne School views online child sexual abuse as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Lead.
- If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead should obtain advice immediately through SPOA or Sussex Police.
- If the school are made aware of incident involving online child sexual abuse of a child then the school will:
    - Act in accordance with the school's child protection and safeguarding policy and the relevant Pan Sussex Child Protection and Safeguarding Procedures.
    - Immediately notify the designated safeguarding lead.
    - Store any devices involved securely.

- Immediately inform East Sussex police via 101 (using 999 if a child is at immediate risk)
- Where appropriate the school will involve and empower children to report concerns regarding online child sexual abuse e.g. or by using the Click CEOP report form: CEOP Safety Centre.
- Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).
- Make a referral to children's social care (if needed/appropriate).
- Put the necessary safeguards in place for pupil(s) e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.
- Inform parents/carers about the incident and how it is being managed.
- Review the handling of any incidents to ensure that the school is implementing best practice and the school leadership team will review and update any management procedures where necessary.

- The school will take action regarding online child sexual abuse regardless of the use of school equipment or personal equipment, both on and off the school premises.
- The school will ensure that all members of the community are aware of sources of support regarding online child sexual abuse.
- If pupils at other schools are believed to have been targeted then the school will seek support from SPOA to enable other schools to take appropriate action to safeguarding their community.
- The school will ensure that the Click CEOP report button is visible and available to pupils and other members of the school community, for example including the CEOP report button the school website homepage and on intranet systems.

9.3. Responding to concerns regarding Indecent Images of Children (IIOC)

It is an offence to possess, distribute, show and make indecent images of children. Making of and distributing indecent images of children includes printing and viewing them on the internet otherwise known as 'downloading'

- Bourne School will ensure that all members of the community are made aware of the criminal nature of Indecent Images of Children (IIOC) including the possible consequences.
- The school will take action regarding of Indecent Images of Children (IIOC) regardless of the use of school equipment or personal equipment, both on and off the premises.
- The school will take action to prevent access accidental access to of Indecent Images of Children (IIOC) for example using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list, implementing appropriate web filtering, implementing firewalls and anti-spam software.
- If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately through SPOA and/or Sussex Police.

- If the school is made aware of Indecent Images of Children (IIOC) then the school will:
  - Act in accordance with the school's child protection and safeguarding policy and the relevant Pan-Sussex Child Protection and Safeguarding procedures.
  - Immediately notify the school Designated Safeguard Lead.
  - Store any devices involved securely.
  - Immediately inform appropriate organisations e.g. the Internet Watch Foundation (IWF), East Sussex police via 101 (using 999 if a child is at immediate risk) and/or the LADO (if there is an allegation against a member of staff).

- If the school are made aware that a member of staff or a pupil has been inadvertently exposed to indecent images of children whilst using the internet then the school will:
  - Ensure that the Designated Safeguard Lead is informed.

- Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via IWF .
- Ensure that any copies that exist of the image, for example in emails, are deleted.

- If the school are made aware that indecent images of children have been found on the school's electronic devices then the school will:
  - Ensure that the Designated Safeguard Lead is informed.
  - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via IWF .
  - Ensure that any copies that exist of the image, for example in emails, are deleted.
  - Inform Sussex police via 101 (999 if there is an immediate risk of harm) and children's social services (as appropriate).
  - Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.

- If the school are made aware that a member of staff is found in possession of indecent images of children on their electronic device provided by the school, then the school will:
  - Ensure that the Designated Safeguard Lead is informed or another member of staff in accordance with the school whistleblowing procedure.
  - Contact the police regarding the images and quarantine any devices involved until police advice has been sought.
  - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with the schools managing allegations policy.
  - Follow the appropriate school policies regarding conduct.

9.4. Responding to concerns regarding radicalisation and extremism online

- The school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in schools and that suitable filtering is in place which takes into account the needs of pupils.
- When concerns are noted by staff that a child may be at risk of radicalisation online then the Designated Safeguarding Lead (DSL) will be informed immediately and action will be taken in line with the school safeguarding policy.
- Online hate content directed towards or posted by specific members of the community will be responded to in line with existing school policies, including anti-bullying, behaviour etc. If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately via the SLES Safeguarding Team and/or East Sussex Police.

9.5 Responding to concerns regarding cyberbullying

Online or cyberbullying can be defined as the use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone.

- Cyberbullying, along with all other forms of bullying, of any member of Bourne School community will not be tolerated. Full details are set out in the school policies regarding anti-bullying and behaviour.
- All incidents of online bullying reported will be recorded.
- There are clear procedures in place to investigate incidents or allegations and support anyone in the school community affected by online bullying.
- If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately through Sussex Police.
- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.

- The school will take steps to identify the bully where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the schools e-Safety ethos.
- Sanctions for those involved in online or cyberbullying may include:
    - Those involved will be asked to remove any material deemed to be inappropriate or offensive.
    - A service provider may be contacted to remove content if those involved refuse to or are unable to delete content.
    - Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour policy or Acceptable Use Policy.
    - Parent/carers of pupils involved in online bullying will be informed.
    - The Police will be contacted if a criminal offence is suspected.

9.6 Responding to concerns regarding online hate

Hate crimes are any crimes that are targeted at a person because of hostility or prejudice towards that person's:

- disability
- race or ethnicity
- religion or belief
- sexual orientation
- transgender identity

9.6.1 Schools must ensure that they respond appropriately regarding online hate and discrimination and support members of the community who may be targeted online.

9.6.2 Online hate at Bourne School will not be tolerated. Further details are set out in the school policies regarding anti-bullying and behaviour.

9.6.3 All incidents of online hate reported to the school will be recorded.

9.6.4 All members of the community will be advised to report online hate in accordance with relevant school policies and procedures e.g. anti-bullying, behaviour etc.

9.6.5 The Police will be contacted if a criminal offence is suspected. If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately through the Sussex Police.

10 Monitoring and reviewing the online safety policy

10.1 The Designated Safeguarding Lead (DSL) is **Claire Munro.**

10.2 The School Online Safety Lead for the Governing Body is **Chiara Potenza.**

10.3 The School Online Safety Champion is **Alex Brown.**

10.4 The effectiveness of this policy and its accompanying schemes of work are subject to evaluation and review on a regular basis by the Head Teacher, Designated Safeguarding Lead, Online Safety Champion and Online Safety Lead for the Governing Body.

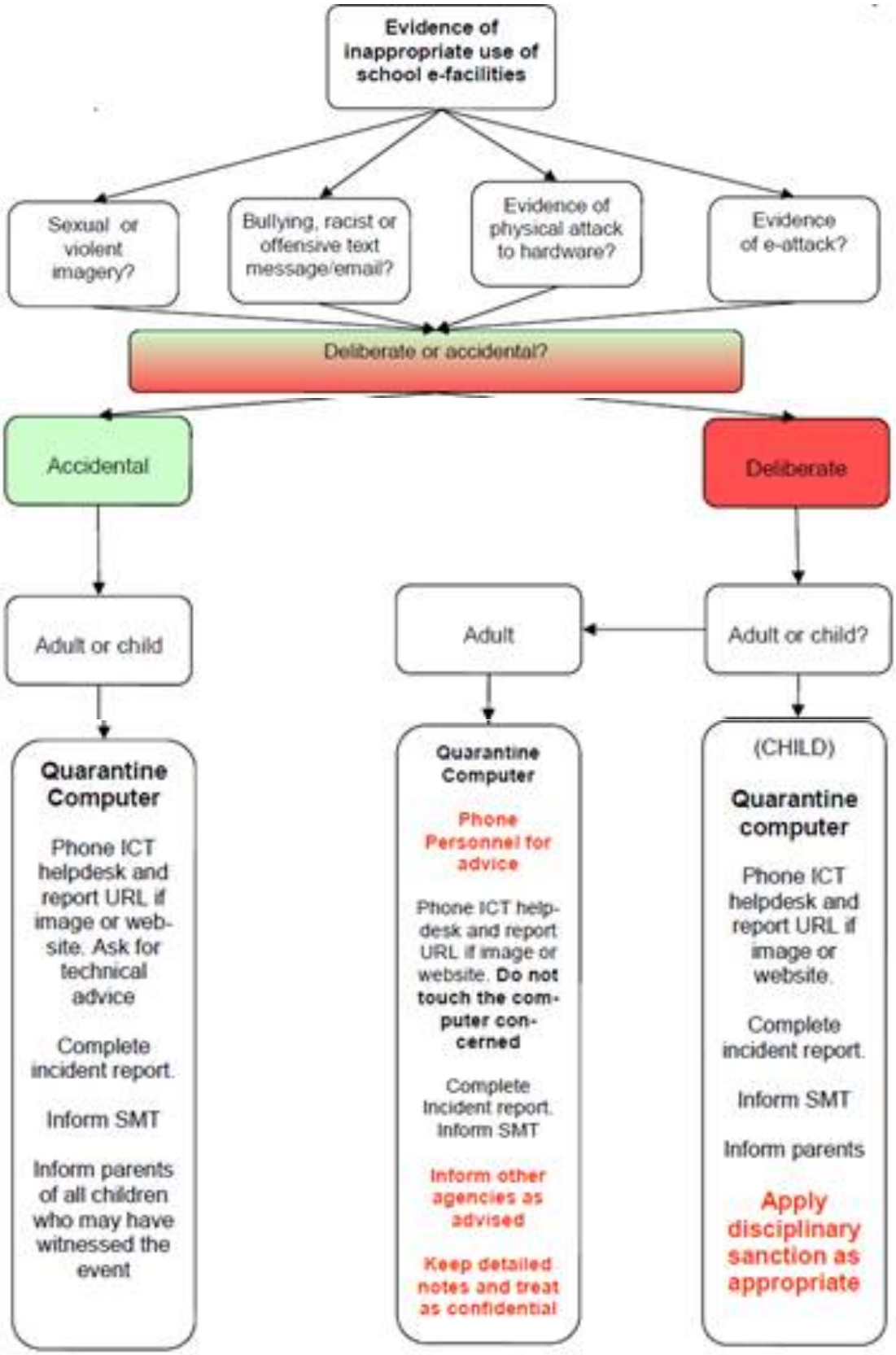
10.5 This policy is monitored on a day-to-day basis by the headteacher, who reports to the Governing Body about its effectiveness

10.6 This policy will be formally reviewed on an annual basis.

Sources

Policy compiled by Alex Brown using ESCC guidelines.

APPENDIX 1: ESCC FLOW CHART



APPENDIX 2: ESCC E-SAFETY REPORT FORM

E-safety Incident	**Acceptable Use Incident**	(Delete as appropriate)	Date	Time	
Name of member of staff (Discovering the incident)					
Child(ren) involved. (Or other adults if no children involved)					
Nature of incident	Accidental access to Inappropriate material	Intentional access to inappropriate Material	Cyber Bullying	Grooming	Other
Details					
The event occurred	During a lesson	In unsupervised time	Outside school hours		
Does the event warrant direct Police involvement? (YES if…)	Grooming	Violent image(s)	Pornographic image(s)	Other criminal activity	

Head Teacher/Deputy Head					
(Staff)	Personnel Contact made with	Recommended action	Action applied	C o Govs	
Other					
Children	Contacted Parents	Date		Time	
	Interviewed Parents/ Carers	(Append notes of interview) Treat as Pink Minute			
File FOUR copies	Top Copy HT	Second Copy Child Safety Officer	Third Copy Child's file	Personnel File	ESCC LSCB/E-Safety Team

East Sussex LSCB (Local Safeguarding Children Board) E-Safety Group: E-safety@eastsussex.gov.uk

APPENDIX 3: MODEL LETTER TO PARENTS

Date: _____

Dear Parent,

Unacceptable or potentially unsafe information or activity concerning your child has been found on _____ . At Bourne School, we take matters of e-safety very seriously as there have been many cases in the news over the years of children being harmed as a result of their behaviour online. If you haven't spoken to anyone from the school about this matter already, please get in touch with _____ to discuss it. In the meantime, we would like to help your child learn how to take steps to make their personal information secure/delete inappropriate content. Please sign the permission form below to enable us to do this.

Whilst allowing children to manage their own risks on social networking sites is an effective way of ensuring their safety, parents should be aware of the following:

- ☐ Strangers may try to contact or meet with children.
- ☐ Children will be at greater risk of cyberbullying.
- ☐ Children may unwittingly give information which could identify them to a potential paedophile.
- ☐ Children will often not tell their parents about the risky or inappropriate behaviour they are engaging in online.
- ☐ A person setting up an account would usually have to lie about their age.

For further help and advice on e-safety, please visit our e-safety page at www.bourne.e-sussex.sch.uk. (Click on Parents then E-Safety.) To see how to secure a Facebook profile, visit https://en-gb.facebook.com/safety.

Yours sincerely,

I give permission for staff of Bourne School to:

- ☐ take steps to make _____ personal information secure / delete inappropriate content;
- ☐ and conduct follow-up checks of online activity in the future.

- ☐ I understand that security settings may be changed and/or inappropriate content may be deleted.
- ☐ I understand that it is my responsibility to talk to my child about their online activities and ensure that they are using the internet in a safe and responsible way.

Signed: _____ Date: _____

APPENDIX 4: Bourne School Pupil Internet, ICT & VLE Agreement

Please tick the boxes and sign:

- ☐ I have read through this agreement with my child and we agree to these safety measures
- ☐ I agree to the VPE etiquette an understand that there will be sanctions if the rules are broken
- ☐ I consent to photographs and/or videos being used in the following ways:
    - ☐ School Photo Album
    - ☐ School Displays
    - ☐ School Concerts
    - ☐ Exhibitions outside the school
    - ☐ Staff Coursework
    - ☐ Press Releases
    - ☐ School Website
    - ☐ Sports Events/Competitions

Signatures:

Pupil Signature:	Pupil Name:
Class:	Date:

Parent Signature:	Relationship to child:
	Date:

APPENDIX 5: Bourne School STAFF USE OF TECHNOLOGY CODE OF CONDUCT

Introduction

ICT in its many forms - internet, email, mobile devices etc - are now part of our daily lives. It is our duty to ensure that they are used safely and responsibly. All staff, governors and visitors at Bourne School are aware of the following responsibilities:

- ☐ ICT includes a wide range of systems, including mobile phones, digital cameras, laptops and tablets.
- ☐ It is a disciplinary offence to use the school ICT equipment for any purpose not permitted by its owner.
- ☐ No staff, governors or visitors will disclose any passwords provided to them by the school.
- ☐ They are responsible for all activity carried out under their username.
- ☐ They will not install any hardware or software on any school owned device without the Head's permission.
- ☐ Their use of the internet may be monitored and if anything untoward is uncovered, could be logged and used in line with any disciplinary procedures. This includes all school owned devices.
- ☐ If an E-safety incident should occur, staff will report it to the Senior or Deputy Designated Professional for Child Protection as soon as possible.
- ☐ All staff, governors and visitors will only use the school's email / internet / czone etc and any related technologies for uses permitted by the Head or Governing Body. If anyone is unsure about an intended use, they should speak to the Head beforehand.
- ☐ They will ensure that data is kept secure and is used appropriately as authorised by the Head of Governing Body. No passwords should be divulged and memory sticks should also be encrypted.
- ☐ Personal devices must only be used in the context of school business with the explicit permission of the Head. Personal mobile phones or digital cameras must NEVER be used for taking any photographs related to school business. Each class has a digital camera specifically for this purpose. These school cameras must NEVER be used for personal use.
- ☐ All staff, governors and visitors using school equipment will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- ☐ They will only use the approved email system for school business.
- ☐ Images will only be taken, stored and used for purposes within school unless there is parental permission for alternative use. At the start of each year, our parents are asked to sign if they agree to their children's images being used on the website or in the local press. If a parent does not agree to this, the school ensures that their child's photograph is not used. Filming and photography by parents and the wider community at school events, such as sports days and school productions, are not allowed.
- ☐ All staff, governors and visitors will make every effort to comply with copyright and intellectual property rights.
- ☐ They will report any incidents of concern regarding staff use of technology and/or children's safety to the Head of the Deputy Designated Professional in line with our school's safeguarding policy.

I acknowledge that I have received a copy of the Acceptable Use Code of Conduct.

Staff member's signature:	Staff member's name:
	Date:

APPENDIX 6: Non-Compliance Procedures

PUPILS ACTIONS? SANCTIONS

Incident	Refer to class teacher	Refer to Assistant Head	Refer to Headteacher/ Online Safety Lead	Refer to Police	Refer to technical support	Inform Parents
Deliberately accessing or trying to access material that could be considered illegal			x	x	x	x
Unauthorised use of non-educational sites during lessons		x	x		x	
Unauthorised use of mobile phone/ digital camera/ other mobile device	x					
Unauthorised use of social media/messaging apps/ email	x					x
Unauthorised downloading or uploading of files	x					x
Allowing others to access school network/ learning platform by sharing usernames and passwords			x		x	x
Attempting to access or accessing the school network using the account of another pupil	x		x			
Attempting to access or accessing the school network using the account of a member of staff	x		x			
Corrupting or destroying the data of other users		x			x	
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		x	x		x	x
Continued infringements of the above, following previous warnings or sanctions			x	x	x	x
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			x			x
Using proxy sites or other means to subvert the school's filtering system			x			x
Accidentally accessing offensive or pornographic material and failing to report the incident	x					
Deliberately accessing or trying to access offensive or pornographic material			x		x	x
Receipt or transmission of material that infringes the copyright of another person or infringes the data protection act			x		x	x

STAFF **ACTION/ SANCTIONS**

Incident	Refer to Assistant Head	Refer to Headteacher	Refer to Local Authority/ HR	Refer to Police	Refer to technical support
Deliberately accessing or trying to access material that could be considered illegal		**x**	**x**	**x**	
Inappropriate personal use of the internet/social media/ personal email	**x**				
Unauthorised downloading or uploading of files		**x**			
Allowing others to access school network/ learning platform by sharing usernames and passwords or attempting to access or accessing the school network, using another person's account		**x**			
Careless use of personal data e.g. holding or transferring data in an insecure manner	**x**				
Deliberate actions to breach data protection or network security rules		**x**			
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		**x**			
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	**x**				
Using personal email/ social networking / instant messaging/ text messaging to carry out digital communications with pupils		**x**			
Actions which could compromise the staff member's professional standing	**x**				
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	**x**	**x**			
Using proxy sites or other means to subvert the school's filtering system	**x**				**x**
Accidentally accessing offensive or pornographic material and failing to report the incident	**x**	**x**			

Deliberately accessing or trying to access offensive or pornographic material		**x**	**x**		
Breaching copyright or licensing regulations		**x**			
Continued infringements of the above, following previous warnings or sanctions		**x**			

APPENDIX 7: FURTHER GUIDANCE

ESCC E-Safety Booklets
https://czone.eastsussex.gov.uk/schoolmanagement/ict/e-safety/Pages/esafetybooklets.aspx
East Sussex LSCB E-Safety Group
E-safety@eastsussex.gov.uk
The Byron Report
http://www.dcsf.gov.uk/byronreview/pdfs/Final%20Report%20Bookmarked.pdf
The Byron Report. Children's Summary
http://www.dcsf.gov.uk/byronreview/pdfs/A%20Summary%20for%20Children%20and%20Young%20People%20FINAL.pdf
The Byron Report Executive Summary
http://www.dcsf.gov.uk/byronreview/pdfs/Executive%20summary.pdf
UK Council for Child Internet Safety (UKCCIS)
http://www.education.gov.uk/ukccis
Child Exploitation and Online Protection (CEOP) Centre
http://www.thinkuknow.co.uk/
Click Clever Click Safe
https://www.education.gov.uk/publications/standard/publicationdetail/page1/DCSF-01100-2009