eSafeguarding Policy

(Incorporating the Cyberbullying, Sexting and IT Acceptable Use Agreements)

January 2018 – January 2019

Reviewed by: Full Governing Body
Coordinator: Anna Lippa
Date: February 2018
Review Date: Annually

This policy is to be read in conjunction with Bowmansgreen's Safeguarding Policy, Anti-bullying (Safe to Learn) policy, Staff Code of Conduct and Behaviour Policy.

Introduction

Bowmansgreen Primary School is committed to providing an e-safe learning environment for all pupils and staff. On-line technology is now commonplace in schools, as part of the learning environment and curriculum, to stimulate and enhance teaching and learning. This shift in internet use not only provides greater creativity but also presents new and increased risks.

This policy ensures that safety measures are in place to protect both pupils and staff against harmful risks that may be faced when learning and working on-line. Our responsibility is to set high expectations of all users of the internet and to maintain a consistent approach to safeguarding on-line.

Aims

In accordance with school procedures for safeguarding children (see Child Protection Policy), locally agreed interagency procedures and the Education Act 2002, and Keeping Children Safe in Education as amended September 2016, the aims of this policy are:

- To ensure that pupils know how to keep themselves safe online
- To safeguard and protect the children and staff of Bowmansgreen
- To ensure that all staff and other stake holders know the potential risk factors online
- To set out the key expectations of all members of the school community with respect to the use of computing-based technologies
- To assist school staff working with children to work safely and responsibly with the internet and other communication technologies
- To assistant staff to monitor their own standards and practice on-line
- To set clear expectations of behaviour and/or codes of practice relevant to the responsible use of the internet for educational, personal or recreational use
- To ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken
- To minimise the risk of misplaced or malicious allegations made against adults who work with pupils

Scope of Policy

- This policy applies to the whole school community including, all staff, volunteers, staff employed indirectly by the school, governors and all pupils
- The Senior Leadership Team and governors will ensure that any relevant or new legislation that may impact upon the provision for eSafeguarding within the school will be reflected within this policy
- The Education and Inspections Act 2006 empowers the Headteacher, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary sanctions for inappropriate behaviour. This is pertinent to

incidents of cyberbullying, sexting, or other eSafeguarding-related incidents covered by this policy, which may take place out of school, but the ability to regulate and/or impose disciplinary penalties are linked to the pupils' membership of the school

- The school will clearly detail its management of incidents within this policy and will, where known, inform parents and carers of incidents of inappropriate eSafeguarding behaviour that takes place out of school
- This policy should be read together with the Social Media Policy, Data Protection Policy, Safe to Learn Policy and Staff Code of Conduct.

4. Roles and responsibilities

At Bowmansgreen, we believe that eSafeguarding is the responsibility of the whole school community and that everyone has a responsibility to ensure that all members of the community are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

4.1 Responsibilities of the Senior Leadership Team

- The Headteacher is ultimately responsible for eSafeguarding provision for all members of the school community
- The Headteacher shares the Child Protection and Safeguarding role with the Deputy Designated Safeguarding/Senior Persons (DSP). All safeguarding issues will be dealt with following the procedures within this policy and the Child Protection policies. The DSPs are the first point of contact in school for all safeguarding matters
- The Headteacher and Senior Leadership Team are responsible for ensuring that all relevant staff receive suitable training to enable them to carry out their eSafeguarding roles
- The DSPs should ensure that they are aware of procedures to be followed in the event of a serious eSafeguarding incident

4.2 Responsibilities of the Computing Subject Lead

- To promote an awareness and commitment to eSafeguarding throughout the school
- To take day-to-day responsibility for eSafeguarding within school and to have a leading role in establishing and reviewing the school eSafeguarding policies and procedures
- To communicate regularly with school technical staff
- To communicate regularly with the Senior Leadership Team
- To provide Governors with an annual eSafeguarding update
- To ensure that eSafeguarding education is embedded across the curriculum in a way which educates children in responsible internet use and digital literacy in an educative, responsible, non-suppressive way
- To raise the level of awareness about safety matters with parents to ensure that the aims of the eSafeguarding Policy are fulfilled at school and home, and to help arm parents with the knowledge and confidence to help keep their children safe online

4.3 Responsibilities of teachers, teaching assistants and support staff

- To read, understand and help promote the school's eSafeguarding policy and guidance
- To read, understand and adhere to the school Staff IT Acceptable Use Policy
- To report any suspected misuse or concern to the Head or DSPs
- To model safe and responsible behaviours in their own use of technology
- To ensure that any digital communications with pupils should be on a professional level and only through school-based systems, NEVER through personal mechanisms, e.g. email, text, mobile phones etc
- To embed eSafeguarding expectations and messages wherever they can when, using technology to support children's learning, whether that learning happens at school or home
- To understand and use school incident-reporting mechanisms and systems
- To supervise and guide pupils carefully when engaged in learning activities involving technology
- To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
- To be aware of eSafeguarding issues and their responsibilities related to the use of mobile phones, cameras and handheld devices
- To safeguard and manage their own online reputation by ensuring that privacy settings of any social media platforms they use are secure and checked frequently.
- To maintain a professional level of conduct in personal use of technology at all times to help maintain public confidence in the profession
- To use all school hardware responsibly

4.4 Responsibilities of technical staff

- To report any eSafeguarding related issues that come to their attention to a DSP
- To develop and maintain an awareness of current eSafeguarding issues, legislation and guidance relevant to their work
- To support the school in providing a safe technical infrastructure to support learning and teaching
- To ensure that access to the school network is only through an authorised, restricted mechanism
- To ensure that provision exists for misuse detection and malicious attack
- To be responsible for the security of the school IT system
- To restrict all administrator level accounts appropriately
- To ensure that access controls exist to protect personal and sensitive information held on school-owned devices
- To ensure that appropriate physical access controls exist to control access to information systems and telecommunications equipment situated within school
- To ensure that appropriate backup procedures exist so that critical information and systems can be recovered in the event of unforeseen data loss or critical incident

5. Communication of the policy

- The e-safeguarding policy will be provided to and discussed with all members of staff formally and training given to ensure they understand and implement it
- All amendments will be updated on the system and awareness sessions will be held for all members of the school community, including parents
- An e-safety module is included across the Computing curriculum
- Pertinent points from the school eSafeguarding policy will be reinforced across the curriculum and across all subject areas when using IT equipment within school
- The key messages contained within the eSafeguarding policy will be reflected and consistent within all acceptable use policies in place within school
- All staff will endeavour to embed eSafeguarding messages across the curriculum whenever the internet or related technologies are used
- Pupils will be encouraged to discuss matters linked to their online safety

6. Managing Digital Content

Thought must be given whenever images, video and sound, including the use of school-generated assets and those found on the internet, are used in school. In order to protect our pupils, we need to be careful when sharing these images, videos and sounds online, e.g. on the website or through the newsletter. In addition, pupils should be taught to think about how they share images, video and sound online in their personal lives.

Written permission from parents or carers will be obtained for the following locations (listed below) before photographs or video of pupils are published. This is done as part of the home-school agreement on entry to the school. Parents and carers may withdraw permission, in writing, at any time. Written requests must be given by both parents or one in a single-parent household, in order for it to be deemed valid.

- On the school website
- On the school's Intranet
- In EYFS, when using the online learning journal: Tapestry
- On the school's Twitter account
- In the school's newsletter
- In the school prospectus and other printed promotional material
- In display material that may be used around the school
- When images are recorded or transmitted on a video or via webcam in an educational conference or for information, demonstration or promotional material on the school website
- We will remind pupils of safe and responsible behaviour when creating, using and storing digital images, video and sound
- We will remind pupils of the risks of inappropriate use of digital images, video and sound in their online activities both at school and at home.
- Pupils and staff will only use school equipment to create digital images, video and sound. In exceptional circumstances and upon the completion of a risk assessment, personal equipment may be used with permission from the Senior Leadership Team, provided that any media is transferred solely to a school device and deleted from any personal devices at the earliest possible opportunity. In

particular, digital images, video and sound will not be taken without the permission of participants; images and video will be of appropriate activities and participants will be in appropriate dress; full names of participants will not be used either within the resource itself, within the file name or in accompanying text online; such resources will not be published online without the permission of the staff and pupils involved

- If pupils are involved, relevant parental permission will also be sought before resources are published online
- Parents may take photographs at school events. However, they must ensure that any images or videos taken involving children other than their own are for personal use only and will not be published on the internet including social networking sites unless permission is sought
- When searching for images, video or sound clips, pupils will be taught about copyright and acknowledging ownership.

6.1 Storage of images

- Any images, videos or sound clips of pupils must be stored on the school network picture drive and never transferred to personally owned equipment
- Pupils and staff are not permitted to use personal portable media for storage of any images, videos or sound clips of pupils
- Class teachers have the responsibility of deleting images relating to their class or year group when they are no longer required, or when a pupil has left the school. The Computing Lead has the responsibility of checking that images are being deleting on a regular basis and has overall responsibility for deleting images of past pupils and staff.

7. Teaching and Learning

- At Bowmansgreen, we believe that the key to developing safe and responsible behaviours online, not only for pupils but everyone within our school community, lies in effective education. We know that the internet and other technologies are embedded in our pupils' lives, not just in school but outside as well, and we believe that we have a duty to help prepare our pupils to safely benefit from the opportunities the internet brings.
- We will provide a series of specific eSafeguarding-related lessons in every year group as part of the computing curriculum
- We will celebrate and promote eSafeguarding through a planned programme of assemblies and whole-school activities, including promoting Anti-Bullying Week (November) and Safer Internet Day (February) each year
- We will discuss, remind or raise relevant eSafeguarding messages with pupils routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use and the need to respect and acknowledge ownership of digital materials
- Any Internet use will be carefully planned to ensure that it is age appropriate and supports the learning objectives for specific curriculum areas

- User generated content (e.g Youtube) must be carefully scrutinised by teachers prior to the lesson it is intended for. Any pop –ups, banner adverts or preliminary ads that appear before the start of the video and are deemed inappropriate will make the video or image unsuitable for use and must be discarded. Access to Youtube will be limited only to teacher's desktop computers, laptops and ipads
- Pupils will be taught how to use a range of age-appropriate online tools in a safe and effective way
- We will remind pupils about their responsibilities through an Acceptable Use Policy which every Key Stage 1 and 2 pupil will sign at the beginning of each academic year (**See Appendix 2**)
- Staff will model safe and responsible behaviours in their own use of technology during lessons
- We will teach pupils how to search for information and to evaluate the content of websites for accuracy when using them in any curriculum area
- When searching the Internet for information, pupils will be guided to use age-appropriate search engines. All use will be monitored and pupils will be reminded of what to do if they come across unsuitable content
- Children will use age appropriate search engines that provide easy access to digital content. When performing search related tasks a variety of suitable search engines must be used in order to differentiate access to online content: KS1 Kiddle.co.uk, KS1and KS2 Swiggle.co.uk, KS2 Google (guided search) and or the use of its safe search filters through HfL
- All pupils will be taught, in an age-appropriate way, about copyright in relation to online resources and will be taught to understand about ownership and the importance of respecting and acknowledging copyright of materials found on the Internet
- Pupils will be taught about the impact of cyberbullying and know how to seek help if they are affected by any form of online bullying
- Pupils will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent or carer, teacher or trusted staff member, or an organisation such as the CEOP and 'report abuse' buttons

7.1 Staff training

- Staff will receive regular information and training on esafeguarding issues in the form of INSET and staff meetings and briefings
- All new staff receive information and guidance on the school's eSafeguarding and Acceptable Use policies as part of the induction process
- All staff will be made aware of individual responsibilities relating to the safeguarding of children within the context of esafeguarding and know what to do in the event of the misuse of technology by any member of the school community
- All staff are encouraged to incorporate esafeguarding activities and awareness within their curriculum areas

8. Communicating safely and securely

8.1 Passwords

Passwords are an important aspect of computer security. They are the front line of authentication for the protection of user accounts and their associated access to IT equipment and resources. A poorly chosen password may result in the compromise of pupil work, progress or assessment information, staff personal or professional, confidential information, sensitive information being lost or stolen or the school's network being infected or attacked.

- A secure and robust username and password convention exists for all system access (email, network access, school management information system (SIMS)
- EYFS and Y1 pupils will have a generic log-in. All pupils in Y2-Y6 have a unique login to access all school computing equipment
- All staff will have a unique, individually-named user account and password for access to IT equipment and information systems available within school
- Staff should be reminded and encouraged to change their passwords at any time that they feel their password may have been compromised
- All staff and pupils have a responsibility for the security of their username and password. Users must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security
- All staff and pupils will be made aware of the importance of protecting access to their personal username and passwords for computing access
- All staff will read and agree to an Acceptable Use Policy and all Key Stage 1 and 2 pupils will sign an Acceptable Use Policy prior to being given access to IT systems
- Staff and pupils will be reminded of the importance of not writing down system passwords
- All staff and pupils will be reminded only to disclose their personal passwords to senior members of staff and authorised computing staff when necessary and never to anyone else. All personal passwords that have been disclosed should be changed as soon as possible
- All users should always use their own personal passwords to access computer based services
- All access to school information assets will be controlled via username and password
- No user should be able to access another user's files unless delegated permission has been granted
- Access to personal data is securely controlled in line with the school's Data Protection and Freedom of Information policies
- A technician may exercise his or her right to refuse to enter a user's password on devices owned by pupils or staff, in accordance with current legislation
- Passwords should contain a combination of numbers, letters, and special characters and be difficult to guess - the more randomly they are placed, the more secure they are
- Users should create different passwords for different accounts and applications
- Lessons will be given to children about how to select appropriate passwords and keep them safe

8.2 Internet Access – Filtering, Monitoring and Alerting

The Internet is a valuable tool for teaching and learning. Unfortunately, not all content that is available on the Internet is suitable for schools, so provision has to be made to ensure that a suitable, fit-for-purpose Internet filtering solution is deployed without 'over-blocking.' At Bowmansgreen, we need to ensure that all users have an appropriate, productive, enjoyable and a safe on-line experience.

- Bowmansgreen uses a filtered and monitored internet service. The filtering system is provided through Hertfordshire Internet and Connectivity Services (HICS) by RM and is called RM SafetyNet
- Bowmansgreen's internet provision includes filtering, monitoring and the alerting of online activity, appropriate to the age and maturity of pupils
- The filtering system uses four standard filters but there is also custom filtering for both websites and searches
- Standard monitoring and reporting is already active on RM SafetyNet
- Searchable reports are available to monitor and investigate internet use: by the whole staff, down to individual users
- There are three different types of alert available:
    - Internet Watch Foundation (IWF) alert – monitoring and alerting access (or attempts to access) child sexual abuse content
    - Prevent Alerts – monitoring and alerting of extremist content
    - Custom alerts – customised by the school
- Alerting: Internet Watch Foundation (IWF)
    - It is illegal to access or seek out child sexual abuse content
    - Uses hidden IWF lists
    - Cannot be overridden or changed in school
    - This alert currently goes straight to RM. They will contact HfL and there will be police involvement
- If a user discovers a website with inappropriate content, this must be documented on the school's concern form and reported to the computing Lead and a DSP
- Bowmansgreen will regularly review the effectiveness of RM SafetyNet and any alerts that are generated by users
- The evaluation of online content materials is part of teaching and learning in every subject and will be viewed as a whole-school requirement, responsibility and expectation across the curriculum

8.3 Internet Access Authorisations

Bowmansgreen allows Internet access to staff and pupils on the grounds that it is required for either work-related purposes or for educational need. However, the school does have provision and procedures in place to remove access for individual users should it become necessary.

- All pupils will have the appropriate awareness training prior to being granted internet access within school
- All KS1 and KS2 pupils will be required to sign the Acceptable Use Policy annually and discuss it on a regular basis with their parents annually

- Staff will always be proactive regarding the nature of content, which can be viewed through the school's internet provision
- The school will maintain a current record of all staff and pupils who have been granted access to the school's internet provision
- Pupils will be closely supervised and monitored during their use of the internet. Pupils will be frequently reminded of internet safety issues and safe usage

9. Email

Electronic mail (email) is an essential communication mechanism for both staff and pupils in today's digitally connected world. The use of email can bring significant educational benefits for any school, both for its staff and pupils. However, email use for staff and pupils needs to be thought through and appropriate safety measures put in place. The unregulated use of email could potentially lead to a safeguarding incident as the more traditional, non-technical access controls can be bypassed with ease.

9. 1 Email Procedures for Staff

- School email should in no way be considered private and its use should be for school-related communication with only limited exceptions.
- Staff should only use approved email accounts allocated to them by the school and should be aware that any use of the school email system may be monitored and checked
- Staff should not use personal email accounts for professional purposes, especially not to exchange any school-related information or documents
- Access, in school, to external personal email accounts may be blocked
- All Bowmansgreen staff have their own email account to use for all school business as a work-based tool. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed
- If parents need to communicate with class teachers via email, they must use the admin@ email account and should expect replies from this account or a member of SLT
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged. A full audit trail can be made available should this become necessary
- School email accounts should be the only account that is used for school-related business
- Staff will only use official school-provided email accounts to communicate with the school community, including pupils, parents, carers and governors
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses

9. 2 Email Procedures Pupils

School email should in no way be considered private and its use should be for school-related communication with only limited exceptions.

- Pupils should only use approved email accounts allocated to them by the school

- Pupils should be aware that any use of the school email system may be monitored and checked
- Pupils will be allocated an individual email account for their own use in school or class
- Pupils may only use school-provided email accounts for school purposes
- Pupils are not permitted to access personal email accounts during school hours
- Whole class or group email addresses will be used in school for communication outside of the school
- Pupils must not access external personal email in school
- Pupils are discouraged from sending or receiving excess social email as this may interfere with their learning and productivity. It will be restricted in line with the school e-safeguarding and Acceptable Use Policies
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged. A full audit trail can be made available should this become necessary
- School email accounts should be the only account that is used for school-related matters

9.3 Email usage

- Pupils may only use school-approved accounts on the school system and only under close teacher supervision
- All users will be reminded about the need to send polite and responsible messages
- All users will be reminded about the dangers of revealing personal information within email conversations
- Pupils will be taught not to reveal personal details of themselves or others in email communications. Pupils will be taught to obtain prior permission from an adult if they arrange to meet with anyone through an email conversation
- Emails to external third parties or agencies that contain personal, confidential, classified or financially sensitive data, need to be controlled and never communicated through the use of a personal account
- All users will be made aware of the dangers of opening email from an unknown sender or source or viewing and opening attachments
- All email and email attachments will be scanned for malicious content
- Users should never open attachments from an unknown or untrusted source - they should consult the network manager first
- Communication between staff , pupils, parents and members of the wider school community should be professional and related to school matters only
- Pupils are taught to adhere to the generally accepted rules of Netiquette; particularly in relation to the use of appropriate language
- Any inappropriate use of the school email system or receipt of any inappropriate messages from another user should be reported to the computing Lead, a member of SLT or a DSP
- All email users within school should report any inappropriate or offensive emails to the computing Lead, a member of SLT or a DSP
- Pupils are encouraged to immediately tell a teacher or trusted adult if they receive any inappropriate or offensive email
- Irrespective of how pupils or staff access their school email (from home or within school), school policies still apply
- Emails sent to external organisations should be written carefully and authorised by a line manager, when necessary, before sending, to protect the member of staff sending the email

- Chain messages will not be permitted or forwarded on to other school-owned email addresses
- The school requires a standard disclaimer to be attached to all email correspondence, stating that, 'the views expressed are not necessarily those of the school'
- All emails should be written and checked carefully before sending, in the same way as a letter written on school-headed paper
- When sending sensitive or important emails to parents or external agencies, staff are advised to carbon copy (cc) the Headteacher, their line manager or another member of SLT into the email where appropriate
- All emails that are no longer required or of any value should be deleted
- Email accounts should be checked regularly for new correspondence (See Staff Code of Conduct)
- When away for extended periods, eg during the school holidays, staff are encouraged to set up an 'out-of-office' notification to remind parents and external organisations that staff are not currently available

10 Mobile Phone Usage

In today's digital world, communications and content are available almost anywhere at any time. Gone are the days when mobile phones could only be used for making phone calls.
As mobile phones have increased in sophistication, with the functionality being almost parallel to that of desktop, laptop and tablet computers, more care has to be taken with the use of smart mobile devices within school. In particular, the ability for mobile phones to connect to the internet via the mobile phone provider, means that pupils, parents and visitors are now able to access, download and upload content on school premises without using the school IT network and the associated safeguards it has in place. These types of devices, if usage is not managed appropriately, pose serious challenges for schools that are trying to safeguard pupil use of the internet within school.

10.1 General Issues

- Pupils are not permitted to bring mobile phones into the classroom
- Mobile phones will not be used during formal lessons, including by staff, visitors and volunteers
- Personal mobile phones must not be used in the classrooms or corridors when children are present – unless previously agreed with SLT
- The use of a mobile phone during the school day is permitted in clearly defined circumstances – see staff Code of Conduct
- Mobile phones and personally owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally owned mobile phones or mobile devices.
- We recommend the Bluetooth function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.
- No images or videos of pupils, staff or parents should be taken on personal mobile phones.
- Wifi access is permitted on devices to visitors of Bowmansgreen

10.2 Pupils' use of mobile phones and other devices

- Pupils are not permitted to bring mobile phones into school except in exceptional circumstances for which permission must be sought by a parent and agreed with a member of SLT.
- All mobile phones will be handed in at reception at the beginning of the school day and locked away. They will only be released again at the end of the day. Any device brought into the classroom will be confiscated
- If a pupil breaches school policy on the acceptable use of mobile phones then the phone or device will be confiscated and will be held in a secure place in the school office; it would then only be released to the pupil's parent or carer
- If a pupil needs to contact a parent or carer, they are to inform their class teacher - or the school office - who will make the decision as to whether it is appropriate or necessary and make the contact on their behalf
- Parents are requested not to try and contact their child via their mobile phone during the school day as it will not be in their child's possession. Contact is to be made via the school office
- Personal mobile phones belonging to pupils are prohibited from any school trip or event.

10.3 Staff use of mobile phones and other devices

- Staff are not permitted to use their own mobile phones or devices for contacting children or their families, within or outside of the school, relating to school business or other members of the school community.
- Within our school community, it is expected that members of staff have friends who are also parents at Bowmansgreen. In such circumstances, staff must adhere to the expectations of confidentiality and professionalism, as set out in the Staff Code of Conduct
- Mobile phones and personally-owned devices will be switched off or switched to 'silent' mode
- Bluetooth communication should be 'hidden' or switched off.
- Staff must not use personal mobiles or have them out in the classrooms or corridors when children are present – unless previously agreed with SLT
- Staff are not permitted to allow children to use their mobile phone as part of an educational activity
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use school provided equipment for this purpose
- All photos taken with an iPad should be stored on the server and not on the device
- Staff may, in exceptional circumstances, use a mobile phone to capture photos/ videos, that do not contain pupils, on a school trip or on-site event
- Staff are prohibited from using iPads to send messages via facetime/imessage or social media platforms during the teaching day
- Where staff members are required to use a mobile phone for school duties, for instance in case of an emergency during off-site activities, or for contacting pupils or parents on a school trip, they should use their own devices and hide (by inputting 141) their own mobile numbers for confidentiality purposes

• If a member of staff breaches this school policy then disciplinary action may be taken, including dismissal.

11 Data Protection and Information Security

Bowmansgreen Primary School holds lots of information and data on pupils, families and on staff. The amount of information which schools hold is increasing all the time and, while this data can be very useful in improving the service and support the school provides, the school has a duty of care for how it handles and controls access to the sensitive and personal information and data which it holds.
The handling of secured data is everyone's responsibility, whether they are an employee, volunteer, technical support or third party provider. Failing to apply appropriate controls to secure data could amount to gross misconduct or even provoke legal action.

- Bowmansgreen Primary School will act and carry out its duty of care for the information assets it holds in line with its Data Protection Act 1998 commitments
- The school will make efforts to ensure that the wider school community understands and support the school's duty of care for the information assets it holds in line with its Data Protection Act 1998 commitments
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998
- The school has deployed appropriate technical, network controls to minimise the risk of data loss or breaches
- All access to personal or sensitive information owned by the school will be controlled appropriately through technical and non-technical access controls
- All computers that are used to access sensitive information should be locked or logged off when unattended
- Users should be vigilant when accessing sensitive or personal information on screen to ensure that no unauthorised users can access or read the information
- All access to information systems should be controlled via a suitably complex password
- All access to the school information management system will be on a need-to-know or least privilege basis
- All information on school servers shall be accessed through a controlled mechanism, with file permissions allocated and assessed on a need to know/ least privilege basis
- Staff and pupils will not leave personal and sensitive printed documents on printers within public areas of the school
- All physical information will be stored in secure, controlled access areas
- Fax machines are only situated within the controlled area of the school office
- All communications involving personal or sensitive information (email, fax or post) should be appropriately secured
- All personal, sensitive and confidential information taken offsite will be secured through appropriate technical controls
- All personal, sensitive and confidential information accessed offsite (e.g via SIMS or CPOMS) will be secured through appropriate technical controls,
- All devices taken off site, e.g. laptops, tablets, removable media or phones, will be secured in accordance with the school's information-handling procedures and, for example, not left in cars or insecure locations

12. Managing IT Systems and Access

- Bowmansgreen will be responsible for ensuring that access to the IT systems is as safe and secure as reasonably possible
- Servers and other key hardware or infrastructure will be located securely with only appropriate staff permitted access
- Servers, workstations and other hardware and software will be kept updated as appropriate.
- Virus and security protection is installed on all appropriate hardware, and will be kept active and up to date

13. Emerging Technologies

As a school we will keep abreast of new technologies and consider both the benefits for learning and teaching and also the risks from an eSafeguarding point of view. We will regularly amend the eSafeguarding policy to reflect any new technology that we use, or to reflect the use of new technology by pupils, which may cause an e-Safeguarding risk.

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before their use in school is allowed
- Bowmansgreen will periodically review which technologies are available within school for any security vulnerabilities that may have been discovered since deployment
- The acceptable use of any new or emerging technologies in use within school will be reflected within the school's eSafeguarding and Acceptable Use policies
- Prior to deploying any new technologies within school, staff, pupils (and if appropriate, parents) will have appropriate awareness training regarding safe usage and any associated risks

14. Preventing Extremism and Radicalisation

Prevent is a strand of the the UK's counter-terrorism strategy. It has been devised to educate pupils about all forms of radicalisation, reduce the threat of terrorism and prevent young people from being drawn into extremist activity. The Counter-Terrorism and Security Act 2015 places a duty on specified authorities, including local authorities and childcare, education and other children's services providers, in the exercise of their functions, to have "due regard to the need to prevent people from being drawn into terrorism" (The Prevent Duty).

There is recognition that the world is online and young people can access thousands of websites from their pockets, anywhere. In this way, young people may be exposed to extremist influences or prejudiced views, in particular those via the internet and other social media. An enormous number of extremist websites exist online that are very easily accessible to young people, thus making it possible for children to be treated as prime targets and groomed online. There is also a risk of children being fed propaganda messages via mobile technologies away from the presence of adults.

Statutory guidance from the DfE issued under Section 175 of the Education Act 2002 ' Keeping Children Safe in Education' (KCSIE) was published in May 2016 for implementation on 5th September 2016. In line with the requirements of the new duty and in addition to our overall Child Protection Policy, we have adopted a child-centred and co-ordinated approach to the new safeguarding requirements.
We continue to take the necessary steps to safeguard our pupils from potentially harmful information or views presented on the internet through the following means:

- Bowmansgreen Primary School and its governing body subscribe to appropriate filtering from HICS using RM SafetyNet. The systems used are 'school safe' and appropriate in accordance with the definition outlined in KCSIE (Annex C, page 61)

- Bowmansgreen, online filtering, monitoring and alerting is carried out though RM SafetyNet.
  - It incorporates the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. This list is maintained by the Counter Terrorism Internet Referral Unit on behalf of the Home Office
  - This filter list is always applied and cannot be overridden by local policy
  - If users attempt to access extremist content covered by this list, then RM will alert the school, including the username where user based filtering has been set up
  - The final escalation process to be followed by RM will be agreed with HfL and documented - school does not enable this

- We employ a sensible, measured and age appropriate approach to filtering so that 'overblocking' the internet is not practiced. We uphold a duty to protect our learners from the dangers of the internet but at the same time teach them the benefits and believe that it is important to prepare them for the real world.

15. Overarching e-safety risks and definitions

Definitions of e-safety issues
The list below is not exhaustive but pertains to relevant and current e-safety issues:

Cyberbullying	1 Cyberbullying is the act of bullying others over the internet or on a mobile phone by sending abusive emails or texts directly or by posting nasty comments or humiliating images for others to see. Cyberbullying is a relatively new form of bullying that describe common forms of bullying such as name- calling, racism, homophobia, sexism etc that happens on-line but like any form of bullying, it can be devastating for the children involved and hard for them to talk about.
Extremism	The UK Government defines extremism as vocal or active opposition to fundamental British values, including democracy, the rule of law, individual liberty and mutual respect and tolerance of different faiths and beliefs. Extremism also includes calls for death of members of the armed forces. (Revised Prevent Duty Guidance for England and Wales (originally issued on 12th March 2015 and revised on 16th July 2015, paragraph 7)
Inappropriate content	It is possible that children may come across things online which are inappropriate for their age and stage of development. In school, filters and restriction settings on particular devices are used to block this content.
Online grooming	Pupils may meet people online who aren't who they say they are, including through online gaming and social media. Grooming is when someone builds an emotional connection with a child to gain their trust for the purposes of sexual abuse, sexual exploitation or trafficking. Children and young people can be groomed online or face-to-face, by a stranger or by someone they know - for example a family member, friend or professional. Groomers may be male or female

	and they could be any age. Many children and young people don't understand that they have been groomed or that what has happened is abuse. Grooming usually takes place over a long period of time. In cases of sexual predators and radicalisation, friendships with unsuspecting children are built up over a time span of 2-3 years.
Online reputation	The internet keeps a record of everything we do online – the photos we upload, the comments other people make about us and things we buy. This is our online reputation. It is important that children, young people and adults understand how to manage their online reputations, including the long-lasting impact that a negative online reputation can have.
Radicalisation	Radicalisation refers to the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. (Revised Prevent Duty Guidance for England and Wales, issued on 12th March 2015 and revised on 16th July 2015, definition) There is a chance that a child or young person may meet people online or visit websites that could lead them over time to adopt extreme right-wing views, and become radicalised. Curiosity could lead a child to seek out these people. As in the incidence of online grooming, an adult online could befriend a child in order to encourage them to adopt beliefs or persuade them to join groups whose views and actions are considered extreme.
Self-harm	Self-harm is when someone hurts themselves on purpose. It can be a way of dealing with difficult or painful feelings. Self-harm is often understood to be a physical response to an emotional pain of some kind, and can be very addictive. Some of the things people do are quite well known, such as cutting, burning or pinching, but there are many other ways for people to hurt themselves, including abusing drugs and alcohol or having an eating disorder. People who self-harm often say it provides short-term relief to emotional pain. If someone self-harms, it doesn't always mean they're suicidal.
Sexting	Young people increasingly choose to send images and messages to their friends, partners, or even strangers they meet online. Sexting is when someone shares sexual, naked or semi-naked images or videos of themselves or others, or sends sexually explicit messages. If someone is under 18 it's against the law for anyone to take or have a sexual photo of them – even if it is a selfie. Sexting images and messages can be sent using mobiles, tablets, smartphones, laptops - any device that allows you to share media and messages.
Sexual abuse	Sexual abuse is when a child or young person is forced or persuaded to take part in sexual activities - whether or not the child is aware. This doesn't have to be physical contact and it can happen online. Sexual abuse may include non-contact activities, such as involving children look at, or in the production of, sexual images, watching sexual activities, encouraging children to behave in sexually inappropriate ways, or grooming a child in preparation for abuse. The child or young person may not understand that what is happening to them is abuse or that anything is wrong. They may be afraid to speak out. Sexual abuse is not solely perpetrated by adult males. Women and other children also commit acts of sexual abuse.

Appendix 1

eSafeguarding Policy - confirmation of compliance

I hereby confirm that I have read, understood and agree to comply with the school's eSafeguarding Policy.

Name ……..……..……..

Position/Post Held……..….

Signed ……..…… Date ……..……

Once completed, signed and dated, please return this form to the Headteacher.

Appendix 2

IT Acceptable Use Agreement - Pupils

- I will only use IT in school for school purposes
- I will only use my class email address or my own school email address when emailing
- I will only open email attachments from people I know, or who my teacher has approved
- I will not tell other people my passwords
- I will only open/delete my own files
- I will make sure that all online and IT device based contact with other children and adults is responsible, polite and sensible
- I will not look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately
- I will not give out my own or others' details such as name, phone number or home address. I will not arrange to meet someone or send my image unless this is part of a school project approved by my teacher and a responsible adult comes with me
- I will be responsible for my behaviour when using IT because I know that these rules are to keep me safe
- I will not upload or add any images, video, sounds or text that could upset or offend any member of the school community
- I know that my use of IT can be checked and my parent/carer contacted if a member of Bowmansgreen school staff is concerned about my safety
- I will not sign up for any online service unless this is an agreed part of the school curriculum or activity, approved by my teacher
- I will not bring my mobile phone to school as I am not allowed to use it, carry it around or have it in my bag during the school day
- If I forget to leave my phone at home, I will leave it at the school office, otherwise it will be confiscated until the end of the day

Appendix 3

Dear Parent/ Carer

The use of a variety of software and the internet, on a range of digital devices, helps to teach pupils to use technology safely, respectfully and responsibly and to recognise acceptable/unacceptable behaviour. A high-quality computing education helps pupils become digitally literate, equips them for the future workplace and as active participants in a digital world., We expect all children to be safe and responsible when using IT and the internet at Bowmansgreen..

Please read and discuss these acceptable use rules with your child and return the slip at the bottom of this page. We would also ask that you read our eSafeguarding policy. If you have any concerns or would like further explanation or information, please contact the Headteacher or Computing Lead.

Please take care to ensure that appropriate systems are in place at home to protect and support your child's use of mobile phones and other devices, especially when connected to the internet.

✂----------

IT Acceptable Use Agreement - Pupils

We have read and discussed this document with …… (child's name) and we agree to follow and support the rules and expectations of this agreement and to support the safe use of IT and the internet at Bowmansgreen Primary School.

Parent/ Carer Signature ……..……..……..……..…….

Pupil signature ……..……

Class …… Date ……..……

Staff Professional Responsibilities

The HSCB eSafety subgroup group have produced a clear summary of **professional responsibilities related to the use of ICT** which has been endorsed by unions. To download visit http://www.thegrid.org.uk/eservices/safety/policies.shtml

PROFESSIONAL RESPONSIBILITIES

When using any form of ICT, including the Internet, in school and outside school

For your own protection we advise that you:

- Ensure all electronic communication with pupils, parents, carers, staff and others is compatible with your professional role and in line with school policies.
- Do not talk about your professional role in any capacity when using social media such as Facebook and YouTube.
- Do not put online any text, image, sound or video that could upset or offend any member of the whole school community or be incompatible with your professional role.
- Use school ICT systems and resources for all school business. This includes your school email address, school mobile phone and school video camera.
- Do not give out your own personal details, such as mobile phone number, personal e-mail address or social network details to pupils, parents, carers and others.
- Do not disclose any passwords and ensure that personal data (such as data held on MIS software) is kept secure and used appropriately.
- Only take images of pupils and/ or staff for professional purposes, in accordance with school policy and with the knowledge of SLT.
- Do not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Ensure that your online activity, **both in school and outside school**, will not bring your organisation or professional role into disrepute.

You have a duty to report any eSafety incident which may impact on you, your professionalism or your organisation.

For HR support and guidance please contact 01438 844933
For eSafety support and guidance please contact 01438 844893

Appendix 4

Bowmansgreen Sexting Policy

Sexting is when someone shares sexual, naked or semi-naked images or videos of themselves or others, or sends sexually explicit messages. They can be sent using mobile phones, tablets, smartphones, laptops - any device that allows you to share media and messages.
Sexting may also be called:

- trading nudes
- dirties
- pic for pic.

For the purposes of this policy, sexting is simply defined as:

- images or videos generated by children under the age of 18, or of children under the age of 18, that are of an indecent or sexual nature

Many young people see sexting as harmless, but creating or sharing explicit images of a child is illegal, even if the person doing it is a child. A young person is breaking the law if they:

- take an explicit photo or video of themselves or a friend
- share an explicit image or video of a child, even if it's shared between children of the same age
- possess, download or store an explicit image or video of a child, even if the child gave their permission for it to be created.

Once taken and sent, the sender has lost control of any images which could end up anywhere. They could be seen by a child's future employers, their friends or even by child sex offenders. By having in their possession, or distributing, indecent images of a person under 18 on to someone else, many young people are not even aware that they could be breaking the law, as these are offences under the Sexual Offences Act 2003. (CEOP, 2015)

As of January 2016 in England and Wales, if a young person is found creating or sharing images, the police can choose to record that a crime has been committed but that taking formal action isn't in the public interest.

There are many different types of sexting and it is likely that no two cases will be the same. It is necessary to carefully consider each case based on its individual circumstances and context. It is important to apply a consistent approach when dealing with an incident to help protect the pupil, the school and staff. The range of contributory factors in each case also needs to be considered in order to determine an appropriate and proportionate response. All staff should be familiar with this policy.

Steps to take in the case of an incident:

Step 1: Disclosure by a student
Sexting disclosures should follow the normal safeguarding practices and protocols. A student is likely to be very distressed especially if the image has been circulated widely and if they don't know who has shared it, seen it or where it has ended up. They will need pastoral support during the disclosure and after the event. They may even need immediate protection or a referral to social services.
The following questions will help decide upon the best course of action:

- Is the pupil disclosing about themselves receiving an image, sending an image or sharing an image?
- What sort of image is it? Is it potentially illegal or is it inappropriate?
- Are the school child protection and safeguarding policies and practices being followed? For example, is the Designated Safeguarding Person (DSP) on hand and is their advice and support available?
- How widely has the image been shared and is the device in the pupil's possession?
- Is it a school device or a personal device?
- Does the pupil need immediate support and or protection?
- Are there other pupils and or young people involved?
- Do they know where the image has ended up?

This situation will need to be handled very sensitively. Whatever the nature of the incident, safeguarding and child protection policies and practices must be adhered to.

Step 2: Searching a device – what are the rules?
In a school-based context, it is highly likely that the image will have been created and potentially shared through mobile devices. It may be that the image is not on one single device: it may be on a website or on a multitude of devices; it may be on either a school-owned or personal device. It is important to establish the location of the image but it must be acknowledged that this may be distressing for the young person involved and support is likely to be needed.
The revised Education Act 2011 brought to bear significant new powers and freedoms for teachers and schools. The Act gives schools and/or teachers the power to seize and search an electronic device if they think there is good reason for doing so.

A device can be examined, confiscated and securely stored if there is reason to believe it contains indecent images or extreme pornography. When searching a mobile device the following conditions should apply:

- The action is in accordance with Bowmansgreen's child protection
- The search is conducted by the Headteacher or a person authorised by them
- A DSP is present
- The search is conducted by a member of the same sex

If any illegal images of a child are found, staff should consider whether to inform the police. Any conduct involving, or possibly involving, the knowledge or participation of adults should always be referred to the police. If an "experimental" incident is not referred to the police, the reasons for this should be recorded in writing. **The child must always be put first**.

Never

- Search a mobile device even in response to an allegation or disclosure if this is likely to cause additional stress to the student/young person UNLESS there is clear evidence to suggest that there is an immediate safeguarding issue or concern

- Print out any material for evidence
- Move any material from one storage device to another

Always
- Inform the school's Designated Safeguarding Person for child protection (DSP)
- Record the incident on the school's 'cause for concern' form
- Act in accordance with school child protection policy and procedures
- Inform relevant colleagues/senior management team about the alleged incident before searching a device

If there is an indecent image of a child on a website or a social networking site, this must be reported to the site hosting it. Under normal circumstances, the reporting procedures on the respective website would be followed. However, in the case of a sexting incident involving a child or young person where there might be the risk of abuse, the incident should be reported directly to CEOP (www.ceop.police.uk/ceop-report) so that law enforcement can make an assessment, expedite the case with the relevant provider and ensure that appropriate action is taken to safeguard the child.

Step 3 - What to do and not do with the image.
If the image has been shared across a personal mobile device:

Always
- Confiscate and secure the device(s)

Never
- View the image unless there is a clear reason to do so (see Step 2 above)
- Send, share or save the image anywhere
- Allow pupils to do any of the above

If the image has been shared across a school network, a website or a social network:

Always
- Block the network to all users and isolate the image

Never
- Send or print the image
- Move the material from one place to another
- View the image outside of the protocols in the Child Protection and Code of Conduct policies and procedures.

Step 4 - Who to involve
Often, the first port of call for a pupil is a class teacher. Whomever the initial disclosure is made, must act in accordance with the school Child Protection policy, ensuring that a DSP is involved in dealing with the incident.
The DSP should always record the incident. There may be instances where the image needs to be viewed and this should be done in accordance with protocols. The best interests of the child should always come first. If viewing the image is likely to cause additional stress, professionals should make a judgement about whether or not it is appropriate to do so.

Step 5 - Deciding on a response
There may be a multitude of reasons why a pupil has engaged in sexting – it may be due to coercion.
It is important to remember that it won't always be appropriate to inform the police; this will depend on the nature of the incident. However, as a school it is important that incidents are consistently recorded. It may also be necessary to assist the young person in removing the image from a website or elsewhere.

- Act in accordance with the Child Protection Policy
- Store the device securely
- Carry out a risk assessment in relation to the young person
- Make a referral to the LADO (if appropriate)
- Contact the police (if appropriate)
- Put the necessary safeguards in place for the pupil, e.g. they may need counselling support, immediate protection and parents must also be informed
- Inform parents and/or carers about the incident and how it is being managed.

Depending on the nature of the image and the family circumstances of the pupil, communication with parents will need to be handled carefully and sensitively.

Step 6 - Contacting other agencies (making a referral)
If the nature of the incident is high-risk, Childrens' Services should be informed. Depending on the nature of the incident and the response, the local police or CEOP may need to be informed.

Appendix 5

Bowmansgreen Cyberbullying Policy

(from the Safe to Learn policy)

Introduction

Bowmansgreen embraces the advantages of modern technology in terms of the educational benefits it brings. However the school is mindful of the potential for bullying to occur. Central to the School's Safe to Learn policy, is the belief that all pupils have a right to be safe at school and not to be bullied: bullying is always unacceptable. Bowmansgreen also recognises that it must take note of and react to bullying perpetrated outside of school which spills over into the school.

A safe, friendly and nurturing environment in school is necessary for pupils to learn and achieve their potential. Cyberbullying by a pupil directed towards another pupil is conduct that disrupts both a pupil's ability to learn and a school's ability to educate its pupils in a safe environment. There is a moral and legal duty placed on schools to protect their pupils and staff and provide a safe and healthy environment.

What is cyberbullying?
Cyber-bullying is an aggressive, intentional act carried out by a group or individual using electronic forms of contact, repeatedly over time against a victim who cannot easily defend himself/herself.

By cyber-bullying, we mean bullying by electronic media:
- Sending unwelcome texts and instant messages that are threatening or cause discomfort
- Making silent calls or sending abusive messages; or stealing the victim's phone and using it to harass others, to make them believe the victim in responsible
- Using a mobile phone camera to take pictures or videos that cause distress, fear or humiliation.
- Posting threatening, abusive, defamatory or humiliating material on websites, including blogs, personal websites and social networking sites
- Sending threatening or bullying emails. These are often sent using a pseudonym or someone else's name
- Hijacking/cloning e-mail or social media accounts

Cyberbullying is insidious; it can be conducted twenty four hours a day, seven days a week, following children into their private space and outside school hours. It can be anonymous. The audience is large and can be reached rapidly. Unlike other forms of bullying, a single incident can be experienced as a multiple attack – a video posted to a website can be copied to many different sites. Bystanders can become accessories by passing on a humiliating message. Messages on social networking sites remain there to damage social life and friendships.

Safeguards in place
- Mobile phones to be handed in to the school office at the beginning of the school day
- All pupils using the internet have read and signed the Pupils' Acceptable Use Policy
- Restrictions, filtering and monitoring of internet use, e.g. no access to social networking sites during the school day
- Regular monitoring and supervising of internet use by staff
- Parent workshops and regular information sent out to parents regarding online safety

- Annual ‘Safer Internet Day’
- Computing curriculum to include eSafety teaching, advice and information

At Bowmansgreen, we teach pupils about the safe use of online communication and mobile devices as well as the serious consequences of cyberbullying, through PSHE, assemblies and the Computing curriculum. We do not tolerate bullying in any form and reserve the right to take action against those who take part in cyberbullying.

- All bullying is damaging but cyber-bullying and harassment can be invasive of privacy at all times. These acts may also be criminal acts.
- We will support victims and, when necessary, work with the police to detect those involved in criminal acts.
- We have a robust behaviour policy and will use the full range of sanctions and consequences, up to and including exclusion, as consequences for pupils who bully fellow pupils in or outside of school.
- Bowmansgreen will use its power of confiscation where necessary to prevent pupils from committing crimes or misusing equipment.
- All members of the school community are aware they have a duty to bring to the attention of the Headteacher any example of cyberbullying or harassment that they know about or suspect.

Guidance for staff

If you suspect or are told about a cyberbullying incident, follow the procedures outlined below:

Mobile Phones

- Ask the pupil to show you the mobile phone
- Note clearly everything on the screen relating to an inappropriate text message or image, to include the date, time and names
- Make a transcript of a spoken message, again record date, times and names
- Tell the pupil to save the message/image
- Take the pupil to the Headteacher, Deputy Headteacher or other member of SLT
- Inform the school’s DSP, if appropriate
- Transfer the details of the incident to a Bowmansgreen concern form

Computers

- Ask the pupil to show on-screen the material in question
- Ask the pupil to save the material
- Print off the offending material straight away
- Make sure you have got all pages in the right order and that there are no omissions
- Accompany the pupil, taking the offending material, to see the Headteacher, Deputy Headteacher or other member of SLT
- Inform the school’s DSP, if appropriate
- Transfer the details of the incident to a Bowmansgreen concern form

Guidance for pupils

If you believe you or someone else is the victim of cyberbullying, you must speak to an adult as soon as possible. This person could be a parent or carer, teacher, MSA, or the Headteacher.

- Do not answer abusive messages but log and report them
- Do not delete anything until it has been shown to a trusted adult (even if it is upsetting, the material is important evidence which may need to be used later as proof of cyberbullying)

- Do not give out personal IT details (eg passwords)
- Never reply to abusive e-mails
- Never reply to someone you do not know, including when gaming online
- Stay in public areas in chat rooms
- Know how to report something that worries you online

Guidance for parents

It is vital that parents and the school work together to ensure that all pupils are aware of the serious consequences of getting involved in anything that might be seen to be cyber-bullying. At Bowmansgreen, we share and invite discussion about our cyber-bullying policy and the procedures in place to deal with cyberbullying.

- Parents can help by making sure their child understands the school's policy and, above all, how seriously Bowmansgreen takes incidents of cyberbullying
- Parents should also explain to their children the legal issues relating to cyberbullying
- If parents believe their child is the victim of cyberbullying by another pupil in the school, they should save the offending material (if need be by saving an offensive text on their or their child's mobile phone) and make sure they have all relevant information before deleting anything
- Parents should contact the Headteacher or Deputy Headteacher as soon as possible once they have a concern about that cyberbullying is taking place
- Parents can help support their children by discussing, modelling and reinforcing safe online behaviour and practices