Bubwith CP School

Esafety Policy – December 2015

(Written using guidance from YGHFL sample documents)

INTRODUCTION

Whilst the whole school community can benefit from the opportunities provided by the Internet and other technologies used in everyday life, at Bubwith CP School we are committed to keeping our pupils safe. Therefore this policy is designed to compliment the school's overall Safeguarding policies and procedures with a strong focus upon safety in the digital world. The eSafety policy supports this by identifying risks and the steps we are taking to avoid them. It shows our commitment to developing a set of safe and responsible behaviours that will enable us to reduce the risks whilst continuing to benefit from the opportunities. Our expectations for responsible and appropriate conduct are formalised in our Acceptable Use Policies (AUP) which we expect all staff and pupils to follow. As part of our commitment to eSafety we also recognise our obligation to implement a range of security measures to protect the school network and facilities from attack, compromise and inappropriate use and to protect school data and other information assets.

Policy Aims:

- To set out the key principles expected of all members of the school community at Bubwith CP School with respect to the use of ICT-based technologies.
- To safeguard and protect the children and staff Bubwith CP School.
- To assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.
- To set clear expectations of behaviour and/or codes of practice relevant to 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 Bubwith CP School's Senior Leadership Team, school board of governors, all staff employed directly or indirectly by the school and all pupils.

- Bubwith CP School's senior leadership team and school board of governors will ensure that any relevant or new legislation that may impact upon the provision for eSafeguarding within school will be reflected within this policy.

- The Education and Inspections Act 2006 empowers head teachers, to such extent as is reasonable, to regulate the behaviour of students or pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyberbullying, or other eSafeguarding-related incidents covered by this policy, which may take place out of school, but is linked to membership of the school.
- The school will clearly detail its management of incidents within this policy, associated behaviour and anti-bullying policies and will, where known, inform parents and carers of incidents of inappropriate eSafeguarding behaviour that takes place out of school.

Review and ownership

- The school has appointed an eSafeguarding coordinator, Miss Amy Bailiss, who will be responsible for document ownership, review and updates.
- The eSafeguarding policy which has been written jointly by the school eSafeguarding Coordinator, Amy Bailiss, and Interim Headteacher, Mrs Mrs Jill Marshall, is current and appropriate for its intended audience and purpose.
- The school eSafeguarding policy has been agreed by the senior leadership team and is awaiting approval by governors.
- The eSafeguarding policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school.
- The School has a named member of the governing body to take lead responsibility for eSafeguarding-Mr Jim O'Neill.
- All amendments to the school eSafeguarding policy will be discussed in detail with all members of teaching staff.

Communication of the safeguarding policy

- Bubwith CP School's Senior Leadership team will be responsible for ensuring all members of school staff and pupils are aware of the existence and contents of the school eSafeguarding policy and the use of any new technology within school.
- The eSafeguarding policy, once agreed by the governing body, will be provided to and discussed with all members of staff formally.
- All amendments will be published and awareness sessions will be held for all members of the school community.
- The children will be made appropriately aware of their role in safeguarding procedures through the age-related AUP documents and the School Council will be consulted on the content of these documents to ensure the language and vocabulary is appropriate and understandable for the intended audience.
- An eSafeguarding or eSafety module will be included in the PSHE and ICT curricula in the Autumn term of every school year - covering and detailing in an age-approriate manner coverage and any amendments to the eSafeguarding policy.
- An eSafeguarding or eSafety training programme will be established across the school to include a regular review of the eSafeguarding policy.
- Pertinent points from the school eSafeguarding policy will be reinforced across the curriculum and across all subject areas when using ICT 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.
- We endeavour to embed eSafeguarding messages across the curriculum whenever the internet or related technologies are used.
- eSafeguarding posters and AUP agreements will be displayed around the school within the vicinity of technologies to reinforce the messages given during safety lessons .

ROLES AND RESPONSIBILITIES

Responsibilities of the senior leadership team

- The headteacher is ultimately responsible for eSafeguarding provision (including eSafeguarding) for all members of the school community, though the day-to-day responsibility for eSafeguarding will be delegated to the eSafeguarding coordinator.
- Make appropriate resources, training and support available to members of the school community to ensure they are able to carry out their roles with regard to eSafety effectively.
- Support the eSafety coordinator in their work.
- Receive and regularly review eSafety incident logs and be aware of the procedure to be followed should an eSafety incident occur in school.
- Develop and promote an eSafety culture within the school community.
- Promote an awareness and commitment to eSafeguarding throughout the school
- Be the first point of contact in school on all eSafeguarding matters.
- Create and maintain eSafety policies and procedures, with the support of other members of staff.
- Develop an understanding of current eSafety issues, guidance and appropriate legislation.
- Ensure that eSafety education is embedded across the curriculum.
- Ensure that eSafeguarding is promoted to parents and carers.
- Liaise with appropriate staff in school, the local authority, the Local Safeguarding Children Board and other relevant agencies as appropriate.
- Monitor and report on eSafeguarding issues to the senior leadership team as appropriate.
- Ensure that an eSafety incident log is kept up to date.
- *Responsibilities of teachers and support staff*
- Read, understand and help promote the school's eSafeguarding policies and related guidance.
- Read, understand and adhere to the school staff Acceptable Use Policy.
- Develop and maintain an awareness of current eSafety issues and guidance.
- Model safe and responsible behaviours in their own use of technology.
- Embed eSafeguarding messages in learning activities where appropriate.
- Supervise and guide pupils carefully when engaged in learning activities involving technology.
- Be aware of what to do if an eSafety incident occurs.
- Maintain a professional level of conduct in personal use of technology at all times.

Responsibilities of technical staff employed by the Local Authority and Visiting Users

- Read, understand and adhere to the school staff Acceptable Use Policy.
- Report promptly any eSafety related issues that come to your attention to the eSafeguarding coordinator.
- Maintain a professional level of conduct in your personal use of technology at all times.
- Support the school in providing a safe technical infrastructure to support learning and teaching.
- Support the security of the school ICT system.

Responsibilities of pupils

- Read, understand and adhere to the school pupil Acceptable Use Policy (Age appropriate AUPs for KS1 and KS2).
- Help and support the school in the creation of eSafeguarding policies and practices and to adhere to any policies and practices the school creates.
- Know and understand school policies on the use of mobile phones, digital cameras and handheld devices.
- To know and understand school policies regarding cyber bullying.
- Take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home.
- Understand what action they should take if they feel worried, uncomfortable, vulnerable or at risk while using technology in school and at home, or if they know of someone who this is happening to.

Responsibilities of parents and carers

- Help and support the school in promoting eSafeguarding.
- Read, understand and promote the school pupil Acceptable Use Policy with their children.
- Take responsibility for learning about the benefits and risks of using the internet and other technologies that their children use in school and at home.
- Take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Discuss eSafeguarding concerns with their children, show an interest in how they are using technology and encourage them to behave safely and responsibly when using technology.
- Model safe and responsible behaviours in their own use of technology.
- Consult with the school if they have any concerns about their children's use of technology.

Responsibilities of the governing body

- Read, understand, contribute to and help promote the school's eSafeguarding policies and guidance.
- Support the work of eSafeguarding in school in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in eSafeguarding activities.
- Ensure appropriate funding and resources are available for the school to implement its eSafeguarding strategy.

MANAGING DIGITAL CONENT

Using images, video and sound

- Written permission from parents or carers will be obtained before photographs of pupils are published online or in the media. This will be done annually or as part of the home-school agreement on entry to the school.
- Parents and carers may withdraw permission, in writing, at any time. Consent has to be given by both parents in order for it to be deemed valid.
- We will remind pupils of safe and responsible behaviours when creating, using and storing digital images, video and sound. We will remind them of the risks of inappropriate use of digital images, video and sound in their online activities both at school and at home.
- Digital images, video and sound will only be created using equipment provided by the school or a safe/reliable source.
- Staff and pupils will follow the school policy on creating, using and storing digital resources.
- 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.
- When searching for images, video or sound clips, pupils will be taught about copyright and acknowledging ownership.

Storage of Images

- Any images, videos or sound clips of pupils must be stored on the school network 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.

LEARNING AND TEACHING

- Through effective education, we can develop safe and responsible behaviours online for the whole school community. The internet and other technologies are embedded in our pupils' lives at school and home. Therefore, we believe we have a duty to help prepare our pupils to safely benefit from the opportunities the internet brings.
- We will provide specific eSafeguarding-related lessons in specific year groups at the beginning of every school year as part of the ICT and PSHE curriculum.
- We will celebrate and promote eSafeguarding through assemblies and whole-school activities, including promoting Safer Internet Day each year.
- We will discuss, remind or raise relevant eSafeguarding messages with pupils routinely wherever suitable opportunities arise; 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.
- We will remind pupils about their responsibilities to which they have agreed through the Acceptable Use Policy.
- Staff will model safe and responsible behaviour in their own use of technology during lessons.

STAFF TRAINING

- Our staff receive regular information and training on eSafeguarding issues in the form of ad hoc training/refresher sessions as required throughout the year, annual updates and termly staff meetings etc.
- As part of the induction process all new staff receives information and guidance on the eSafeguarding policy and the school's Acceptable Use Policies.
- 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 misuse of technology by any member of the school community.
- All staff will be encouraged to incorporate eSafeguarding activities and awareness within their curriculum areas.

MANAGING ICT SYSTEMS AND ACCESS

- The school will be responsible for ensuring that access to the ICT systems is as safe and secure as reasonably possible.
- Servers and other key hardware or infrastructure will be located securely.
- Servers, workstations and other hardware and software will be kept updated as appropriate.
- Virus protection is installed on all appropriate hardware, and will be kept active and up to date.
- The school leadership team will agree which users should and should not have internet access, and the appropriate level of access and supervision they should receive.
- All users will sign an end-user Acceptable Use Policy provided by the school, appropriate to their age and type of access. Users will be made aware that they must take responsibility for

their use and behaviour while using the school ICT systems and that such activity will be monitored and checked.

- Pupil Internet access will be supervised by a member of staff.
- Members of staff will access the internet using staff accessibility accounts through encrypted personal machines using an individual id and password, which they will keep secure. They will ensure that they log out after each session and not allow pupils to access the internet through their id and password. Members of staff will abide by the school AUP at all times. They will not allow children unsupervised access to their computers.
- Any administrator or master passwords for school ICT systems should be kept secure and available to at least two members of staff.
- The school will take all reasonable precautions to ensure that users do not access inappropriate material. However, it is not possible to guarantee that access to unsuitable material will never occur.
- The school will regularly audit ICT use to establish if the eSafety policy is adequate and that the implementation of the eSafety policy is appropriate. We will regularly review our internet access provision, and review new methods to identify, assess and minimize risks.

EMERGING TECHNOLOGIES

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out by the senior leadership team before their use in school is allowed.
- Emerging technologies can incorporate software and/or hardware products.
- The school 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 eSafeguarding and Acceptable Use policies.
- Prior to deploying any new technologies within school, staff and pupils will have appropriate awareness training regarding safe usage and any associated risks.
- 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 the appropriate authorities.
- In line with the school's anti-bullying policy and the 'Bubwith School Whole School Community Guidelines For The use of Social Networking and On-line Media' document' (see appendix 1), the sending of abusive or inappropriate text, picture or video messages is forbidden.

FILTERING INTERNET ACCESS

- Bubwith CP School uses the Local Authority IT filtering system to ensure that systems to protect children are reviewed and improved.
- The school will always be proactive regarding the nature of content which can be viewed through the school's internet provision.
- If users discover a website with inappropriate content, this should be reported to a member of staff who will inform the eSafeguarding Coordinator. All incidents should be documented.
- If users discover a website with potentially illegal content, this should be reported immediately to the eSafeguarding Coordinator. The school will report such incidents to

appropriate agencies including the filtering provider, the local authority, or any other relevant body including the police.

- Filtering and other security systems will be reviewed to ensure they meet the needs of all users.

EMAIL

- Staff and pupils should only use approved email accounts allocated to them by the school and should be aware that any use of the school email system will be monitored and checked.
- Pupils may only use school-provided email accounts for school purposes and only under direct teacher supervision for educational purposes.
- Pupils are not permitted to access personal e-mail accounts during school.
- Responsible use of personal web mail accounts by staff is permitted.
- School email accounts should be the only account that is used for school-related business.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.
- Pupils and staff will be reminded when using email about the need to send polite and responsible messages, about the dangers of revealing personal information, about the dangers of opening e-mail from an unknown sender, or viewing/opening attachments.
- Any inappropriate use of the school email system or receipt of any inappropriate messages from another user should be reported to a member of staff immediately.
- All emails should be written and checked carefully before sending, in the same way as a letter written on school-headed paper.

PUBLISHING CONTENT ONLINE

- Blogging, podcasting and other publishing of online content by pupils, whilst at School, will take place only on the school website.
- Pupils whilst at School will not be allowed to post or create content on sites unless the site has been approved by a member of the teaching staff.
- No public blogs are run by staff on behalf of the school but if they were to be introduced they would need to be approved by the Headteacher and Esafety Coordinator and Governor and be hosted on the school website with postings being approved by the head teacher before publication.
- Pupils will not use their real name when creating publicly-accessible resources. They will be encouraged to create an appropriate nickname.
- Personal publishing will be taught via age-appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.
- Staff and pupils will be encouraged to adopt similar safe and responsible behaviours in their personal use of blogs, wikis, social networking sites and other online publishing outside school.
- Material published by pupils, governors and staff in a social context which is considered to bring the school into disrepute or considered harmful to, or harassment of another pupil or member of the school community will be considered a breach of school discipline and treated accordingly.

IPAD AND TABLET USAGE IN SCHOOL

- The school has leased iPads to enhance and enrich the curriculum for learners and to provide real-time assessment strategies for teachers.
- Teachers and pupils will use the tablets for educational purposes only.
- Student use of the devices will be carefully supervised and monitored.

MOBILE PHONE USAGE IN SCHOOLS

- Mobile phones and personally-owned electronic devices will not be used in any way during lessons or formal school time.
- Use of mobile phones by pupils on school premises is not permitted, and all mobile phones and personally-owned devices will be handed in at reception should they be brought into school.
- Mobile phones and personally-owned mobile devices brought in to school by adults 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.
- No images or videos should be taken on mobile phones or personally-owned mobile devices by pupils, staff or visitors without the prior consent of the person or people concerned.

DATA PROTECTION AND INFORMATION SECURITY

- The school community will act and carry out its duty of care for the information assets it holds in line with its Data Protection Act 1998 commitments.
- All computers that are used to access sensitive information should be locked when unattended.
- Users should be vigilant when accessing sensitive or personal information on screen to ensure that no one else, who may be unauthorised, can read the information.
- Staff and pupils will not leave personal and sensitive printed documents on printers within public areas of the school.
- Fax machines will be situated within controlled areas of the school.
- All communications involving personal or sensitive information (email, fax or post) should be appropriately secured.
- 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.

MANAGEMENT OF ASSETS

Details of all school-owned hardware will be recorded in a hardware inventory.

Details of all school-owned software will be recorded in a software inventory.

All redundant ICT equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.

Disposal of any ICT equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. (Further information can be found on the Environment Agency website).

Any incidents or failure to comply with this policy and also the Acceptable Use Policies will be dealt with following the school's normal behaviour or disciplinary procedures. Discipline consequences for pupils will be at discretion of the Headteacher.

Instances of cyberbullying will be taken very seriously by the school and dealt with using the schools anti-bullying procedures. School recognises that staff as well as pupils may be victims and will take appropriate action in either situation.

Appendix 1

Bubwith Primary School

Whole School Community Guidelines For The use of Social Networking and On-line Media

This school asks its whole community to promote the 3 commons approach to online behaviour:

- Common courtesy
- Common decency
- Common sense

How can common courtesy be shown online?

- Ask someone's permission before uploading photographs, videos or any other information about them online.
- Do not write or upload 'off-hand', hurtful, rude or derogatory comments and materials. To do so is disrespectful and may upset, distress, bully or harass.

How can common decency be shown online?

- Do not post comments that can be considered as being intimidating, racist, sexist, homophobic or defamatory. This is cyber-bullying and may be harassment or libel.
- When such comments exist online, do not forward such emails, tweets, videos, etc. By creating or forwarding such materials, we are all liable under the law.

How can common sense be shown online?

- Think before you click.
- Think before you upload comments, photographs and videos.
- Think before you download or forward any materials.
- Think carefully about what information you share with others online, check where it is saved and check privacy settings.
- Make sure you understand changes in use of any web sites used.
- Block harassing communications and report any abuse.

Any actions online that impact on the school and can potentially lower the school's (or someone in the school's) reputation in some way are deemed as being inappropriate will be responded to.

In the event that any member of staff, student or parent/carer is found to be posting libellous or inflammatory comments on Facebook or other social network sites, they will be reported to the appropriate 'report abuse' section of the network site. (All social network sites have clear rules about the content which can be posted on the site and they provide robust mechanisms to report contact or activity which breaches this.)

In serious cases we will also consider legal options to deal with any such misuse.