Online safety and procedure policy
Updated Jan 2021 V3: Lockdown
Bretherton Endowed CE Primary School

"Learning together, growing together, achieving together, caring together
within our Christian family"

This policy is for Bretherton Endowed CE Primary School and The Hub, Bretherton Endowed Out of School Provision.
Updated Jan 2020 during National Lockdown

Contents Policy
1. Background/Rationale ..
2. Definitions
3. Associated School Policies and procedures
4. Communication/Monitoring/Review of this Policy and procedures
5. Schedule for Development / Monitoring / Review
6. Scope of the Policy

PROCEDURES
1. Roles and Responsibilities
1.1 Governors
1.2 Head teacher
1.3 Online Safety Coordinator/Designated Safeguarding Lead
1.4 Network Manager/Technical staff
1.5 Learning Platform Leader
1.6 Data Manager
1.7 All Staff
1.8 Pupils
1.9 Parents

2. Training
2.1 Staff and Governor Training
2.2 Parent Awareness and Training

3. Teaching and Learning
3.1 Why Internet use is Important
3.2 How Internet Use Benefits Education
3.3 How Internet Use Enhances Learning
3.4 Pupils with Additional Needs

4. Managing Information Systems
4.1 Maintaining Information Systems Security
4.2 Password Security
4.3 Managing Email

4.4 Emailing Personal, Sensitive, Confidential or Classified Information
4.5 Zombie Accounts
4.6 Managing Published Content
4.7 Use of Digital and Video Images
4.8 Managing Social Networking, Social Media and Personal Publishing Sites
4.9 Managing Filtering
4.10 Managing Emerging Technologies
4.11 Data Protection
4.12 Disposal of Redundant ICT Equipment .

5. Policy Decisions
5.1 Authorising Internet Access
5.2 Assessing Risks
5.3 Unsuitable/Inappropriate Activities
5.4 What are the risks?
5.5 Responding to Incidents of Concern
5.6 Managing Cyber-bullying
5.7 Managing Learning Environment/Platforms
5.8 Managing Mobile Phones and Personal Devices

6. Communicating Policy and procedures
6.1 Introducing the Policy and procedures to Pupils
6.2 Discussing the Policy and procedures with Staff
6.3 Enlisting Parents' Support

7. Complaints

Please ensure that prior to publication, any working Appendices and references to those Appendices in the body of the Policy and procedures are removed.

Appendix A	-	**School Online Safety Audit**
Appendix B	-	**Sample EYFS, Primary and Special School Online Safety Posters**
Appendix C	-	**EYFS, Primary & Special School Pupil Acceptable Use Agreement**
Appendix D	-	**Staff/Volunteer Acceptable Use Agreement**
Appendix E	-	**Social Networking Sites (Facebook) Guidance for Parents**
Appendix F	-	**Response to an Incident or Concern Flow Chart**
Appendix G	-	**Sample Online Safety Incident Log**
Appendix H	-	**Online Safety Links**
Appendix I	-	**Legal Framework**
Appendix J	-	**Glossary of Terms**
Appendix K	-	**Cyberbullying support**

POLICY

At Bretherton Endowed CE Primary School we understand the responsibility we have to educate our pupils on e-safety issues; teaching them appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

We have a whole school approach to the safe use of ICT and creating this safe learning environment includes three main elements:

- an effective range of technological tools
- policies and procedures, with clear roles and responsibilities
- a comprehensive e-safety programme for pupils, staff and parents.

1. Background/Rationale

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use online and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. The school Online Safety Policy and procedures will help to ensure safe and appropriate use. The development and implementation of such a strategy will involve all the stakeholders in a child's education from the Head teacher and Governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the pupils themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put young people at risk within and outside the school.

Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content;
- Unauthorised access to/loss of/sharing of personal information;
- The risk of being subject to grooming by those with whom they make contact on the internet;
- The risk of being targeted by extremists in order to promote and encourage radicalisation;
- The risk of being targeted by those involved in child sexual exploitation;
- The sharing/distribution of personal images without an individual's consent or knowledge;
- Inappropriate communication/contact with others, including strangers;
- Cyber-bullying;
- Access to unsuitable video/internet games;
- An inability to evaluate the quality, accuracy and relevance of information on the internet;
- Plagiarism and copyright infringement;
- Illegal downloading of music or video files;
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this Online Safety Policy and procedures is used in conjunction with other school Policies including the Overarching Safeguarding Statement, Child Protection, Data Protection and Whole School Behaviour.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The Online Safety Policy and procedures that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

School vision for E Safety

At Bretherton, we believe that e-Safety is about promoting the benefits to be gained from using technology safely, respectfully and responsibly whilst taking every reasonable precaution to reduce potential harm.

Through the implementations of an effective e-Safety policy, we strive to establish safeguards and equip all members of our school community with the skills to manage risks carefully. We want our pupils to be are responsible, competent, confident and creative users of information and communication technology (ICT).

By the end of KS1, we want every pupil to:

Be able to use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

By the end of KS2, we want every pupil to:

Be able use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.

2. Definitions

For the purposes of this document a child, young person, pupil or student is referred to as a 'child' or a 'pupil' and they are normally under 18 years of age. Wherever the term 'parent' is used this includes any person with parental authority over the child concerned e.g. carers, legal guardians etc.

Wherever the term 'Head teacher' is used this also refers to any Manager with the equivalent responsibility for children.

3. Associated School Policies and procedures

This Policy should be read in conjunction with the following school Policies/procedures:

- Child Protection Policy
- Data Protection Policy
- Health and Safety Policy and procedures
- Whole School Behaviour Policy
- Code of Conduct for staff and other adults
- Home-School Agreement

4. Communication/Monitoring/Review of this Policy and procedures

This Policy and procedures will be communicated to staff, pupils and the wider community in the following ways:

- Posted on the school website/shared staff drive
- Policy and procedures to be discussed as part of the school induction pack for new staff and other relevant adults including the staff Acceptable Use Agreement
- Acceptable Use Agreements discussed with pupils at the start of each year
- Acceptable Use Agreements to be held in pupil and personnel files

The Online Safety Policy is referenced from within other school Policies and procedures as outlined above.

5. Schedule for Development / Monitoring / Review

This Online Safety Policy and procedures was approved by the Governing Body/Governing Body Committee on:	September 2019 Nov 2020 national lockdown Jan 2021 after national lockdown
The implementation of this Online Safety Policy and procedures will be monitored by the:	Resources and standards Sub-Committee , online safety governor and Headteacher
Monitoring will take place at regular intervals:	Annually
The Governing Body/Governing Body Committee will receive a report on the implementation of the Online Safety Policy and procedures generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	Annually
The Online Safety Policy and procedures will be reviewed in accordance with the Governors decision on frequency, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	September 2021
Should serious Online safety incidents take place, the following external persons/agencies will be informed:	LA/ DO Online leader Designated safeguarding lead Police Online safety governor

The school will monitor the impact of the Policy and procedures using:
- *Logs of reported incidents*
- *Surveys/questionnaires of pupils (e.g. Ofsted "Tell-us" survey/CEOP ThinkUknow survey)*
- *parents*
- *staff*

6. Scope of the Policy

This Policy and procedures applies to all members of the school community (including staff, pupils, volunteers, parents, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Head teachers/Principals, 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 penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online safety related incidents covered by this Policy and procedures, which may take place out of school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for, and of, electronic devices and the deletion of data. In the case of both acts, action can only be taken with regard to issues covered by the published Whole School Behaviour Policy.

The school will deal with such incidents within this Policy and procedures and the Whole School Behaviour Policy which includes anti-bullying procedures and will, where known, inform parents of incidents of inappropriate on-line safety behaviour that take place out of school.

PROCEDURES

1. Roles and Responsibilities

The following section outlines the roles and responsibilities for on-line safety of individuals and groups within the school:

1.1 Governors

The role of the Governors is to:

- ensure that the school follows all current online safety advice to keep the children and staff safe;
- approve the Online Safety Policy and procedures and review its effectiveness. This will be carried out by the Governors/Governors Sub-committee receiving regular information about online safety incidents and monitoring reports.
- support the school in encouraging parents and the wider community to become engaged in online safety activities;
- regular review with the headteacher (including incident logs, filtering/change control logs etc.)

1.2 Head teacher

The Head teacher has overall responsibility for online safety provision and will:

- take overall responsibility for data and data security;
- ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements;
- ensure that the Online Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their online safety roles and to train other colleagues, as relevant;
- ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles;
- receive regular monitoring reports from the Online Safety Coordinator;
- be aware of the procedures to be followed in the event of a serious online safety incident or an allegation being made against a member of staff or volunteer (see flow chart on dealing with online safety incidents – Appendix I, and relevant Local Authority HR/school disciplinary procedures). The procedures for dealing with allegations against staff or volunteers can be found within the school Child Protection Policy and all staff/volunteers are provided with a copy on induction.
- In line with remote learning expectations, the HT and DHT will take overall responsibility of online safeguarding issues associated with remote learning.

1.3 Online Safety Coordinator

The Online Safety Coordinator will:

- take day-to-day responsibility for online safety issues and take a lead role in establishing and reviewing the school online safety procedures and documents;
- promote an awareness and commitment to e-safeguarding throughout the school community;
- ensure that online safety education is embedded across the curriculum;
- liaise with the school ICT technical staff
- communicate regularly with the headteacher and the governing body to discuss current issues, review incident logs and filtering/change control logs;
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident or allegation against a member of staff or volunteer;
- ensure that an online safety log is kept up to date;
- facilitate training and advice for staff and others working in the school;
- be aware of emerging online safety issues and legislation, and of the potential for serious child protection issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate online contact with adults/strangers
- potential or actual incidents of grooming
- cyberbullying and the use of social media

1.4 Network Manager/Technical staff
The school's IT support/broadband providers will:

- report any online safety related issues that arise, to the Online Safety Coordinator;
- ensure that users may only access the school's networks through an authorised and properly enforced password protection procedures, in which passwords are regularly changed;
- ensure that the school's ICT infrastructure is secure and is not open to misuse or malicious attack e.g. keeping virus protection up to date;
- the school's procedures on web filtering, is applied and updated on a regular basis;
- ensure that access controls/encryption exist to protect personal and sensitive information held on school-owned devices;
- that the use of the network/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the Online Safety Coordinator for investigation;
- ensure that appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster and in order to complement the business continuity process;
- keep up-to-date documentation of the school's e-security and technical procedures.

1.5 All Staff
It is the responsibility of all staff to:

- read, understand and help promote the school's Online Safety Policy and procedures
- read, understood and adhere to the school Staff Acceptable Use Agreement;
- be aware of online safety issues related to the use of mobile phones, cameras and hand-held devices and that they monitor their use and implement current school procedures with regard to these devices;
- report any suspected misuse or problem to the Online Safety Coordinator;
- maintain an awareness of current online safety issues and guidance e.g. through CPD opportunities;
- model safe, responsible and professional behaviours in their own use of technology;
- ensure that any digital communications with pupils are on a professional level and only through school-based systems, never through personal mechanisms, e.g. email, text, mobile phones or social media messaging or posts.
- Ensure that when moving to remote learning that they will have consideration for their and their class children's online safety when setting work and interacting online line remotely and will act appropriately with the spirit of this policy.
- Ensure that they feel confident in applyin this policy online.

Teachers must:

- ensure that online safety issues are embedded in all aspects of the curriculum and other school activities;
- monitor, supervise and guide pupils carefully when engaged in ICT activity in lessons, extra-curricular and extended school activities;
- ensure that pupils are fully aware of research skills and are made aware of legal issues relating to electronic content such as copyright laws.

- ensure that during lessons where internet use is pre-planned pupils are guided to sites checked as suitable for their use and that processes are known and used when dealing with any unsuitable material that is found in internet searches.
- ensure that when setting work that requires online searches, they remind children of how to search safelt, which engines, websites to use and support parents in keeping their children safe.
- Ensure that staff remind pupils when working online, of what to do in th eveny of seeing inappropriate material and report to their class teacher if this happens so that we can quickly act to minimise impact.

1.6 Pupils

Taking into account the age and level of understanding, the key responsibilities of pupils are to:

- use the school ICT systems in accordance with the Pupil Acceptable Use Agreement – see Appendix D or E, which they and/or their parents will be expected to sign before being given access to school systems;
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- know and understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- know what action to take if they or someone they know feels worried or vulnerable when using online technology;
- know and understand school procedures on the use of mobile phones, digital cameras and hand-held devices.
- know and understand school procedures on the taking/use of images and on cyber-bullying;
- understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy and procedures covers their actions out of school, if related to their membership of the school;
- take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home;
- tell their parents immediately and teachers at the earliest opportunity if they witness anything inappropriate online so risks can be minimised.
- Use previous online learning to reduce risks taken in learning online.

1.7 Parents

Parents play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Research shows that many parents do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through *parents' evenings, newsletters, letters, website and information about national or local online safety campaigns.*

The key responsibilities for parents are to:

- support the school in promoting online safety which includes the pupils' use of the Internet and the school's use of photographic and video images;
- endorsing (by signature) the Pupil Acceptable Use Agreement – see Appendix D or E;
- access the school website/VLE/online pupil records in accordance with the relevant school Acceptable Use Agreement;
- consult with the school if they have any concerns about their children's use of technology;
- ensure that they themselves do not use the internet/social network sites/other forms of technical communication in an inappropriate or defamatory way;
- support the school's approach to online safety by not uploading or posting to the Internet any pictures, video or text that could upset, offend or threaten the safety of any member of the school community or bring the school into disrepute.

- If remote learning has been set, to monitor use and access to the internet at home and alert school if there is any concerns or safeguarding issues.
- Using Google meets for remote contact, to (where possible) be present in the vicinity of the computer and for our younger children to help facilitate the contact.

2. Training

2.1 Staff and Governor Training
This school:

- ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection;
- makes training available to staff on online safety issues and the school's online safety education programme;
- provides, as part of the induction process, all new staff and volunteers with information and guidance on the Online Safety Policy and the school's Acceptable Use Agreements.

2.2 Parent Awareness and Training
This school seeks to regularly provide advice, guidance and training for parents, including:

- the introduction of the Acceptable Use Agreements, to ensure that principles of e-safe behaviour are made clear;
- the provision of information in the school newsletter and on the school website;
- suggestions for safe Internet use at home;
- the provision of information about national support sites for parents.

School will offer Google meet teaining sessions regularly and will post all training material on our website for use when required.
School will seek to establish satisfaction of remote learning and any safeguarding concerns regularly when learning remotely.

3. Teaching and Learning
3.1 Why Internet use is Important
• The Internet is a part of everyday life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.
• Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.
When remote learning is planned, teachers will make additional consideration as to the relevance and safety of links and website research.
Staff will respond immediately to any concerns regarding safety online as a result of work set.
Staff will remind pupils at least weekly or as lessons dictate as to the importance of learning online and how to be online safely.
During supporting Vulnerable and critical workers in school, our safeguarding and online policy will be reiterated to children within school.
When the vulnerable and critical workers children are in school and accessing google meet, this will be in an open room, with adults supervising within the vicinity.

3.2 How Internet Use Benefits Education
Benefits of using the Internet in education include:
• access to worldwide educational resources including museums and art galleries;
• educational and cultural exchanges between pupils worldwide;
• vocational, social and leisure use in libraries, clubs and at home;
• access to experts in many fields for pupils and staff;

• professional development for staff through access to national developments, educational materials and effective curriculum practice;

• collaboration across networks of schools, support services and professional associations;

• improved access to technical support including remote management of networks and automatic system updates;

• exchange of curriculum and administration data with the Local Authority and DfE;

• access to learning wherever and whenever convenient.

3.3 How Internet Use Enhances Learning
This school incorporates online safety education programme as part of the Computing curriculum/PSHE curriculum. This covers the teaching of a range of skills and behaviours which are appropriate to the age and experience of the pupils concerned and include those to:

- STOP and THINK before they CLICK;
- develop a range of strategies to evaluate and verify information before accepting its accuracy;
- be aware that the author of a website/page may have a particular bias or purpose and to develop skills to recognise what that may be;
- know how to narrow down or refine a search;
- [for older pupils] understand how search engines work and to understand that this affects the results they see at the top of the listings;
- understand acceptable behaviour when using an online environment/email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
- understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
- understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
- understand why they must not post pictures or videos of others without their permission;
- know not to download any files – such as music files – without permission;
- have strategies for dealing with receipt of inappropriate materials;
- [for older pupils] understand why and how some people will 'groom' young people for sexual reasons;
- Understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying;
- Know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the Internet and related technologies, i.e. parent, teacher or trusted staff member, or an organisation such as ChildLine.
- plans Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas;
- will remind pupils about their responsibilities through an end-user Acceptable Use Agreement which will be displayed throughout the school or when they log on to the school's netword.
- ensures staff will model safe and responsible behaviour in their own use of technology during lessons;
- ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights;
- ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying online, online gaming/gambling etc.

3.4 Pupils with Additional Needs

Some pupils may need additional teaching that includes reminders and explicit prompts to link their existing knowledge of "how to keep safe" to the rules that will apply specifically to, for instance, internet use.

3.5 Mobile Devices

At Bretheton, we believe that mobile devices offer a fantastic opportunity to extend the learning experiences of our pupils. We seek to be on the front foot with technology and make the most of new opportunities. Given this approach, we recognise the importance for diligence in seeking to use mobile devices safely and responsibly.

Current provision of iPads in school:

- Each member of staff has access to an iPad/ tablet.
- A half class set of 16 iPads is shared between pupils

'Mobile devices' covers all portable electronic devices which have access to the internet, excluding laptop computers.

During National Lockdown, deviced may be lent to children who have barriers to technology and a loan agreement will be shared and signed by parents.

In anticipation of our 1 to 1 device technology being rolled out, a further review of this online safety policy and acceptable user agreement will be conducted and a new agreement drawn up.

USE OF IPADS

Management and use of staff iPads:

- Staff can connect iPads to the school Wifi network to use apps, to email and to access the internet.
- Staff have permission to download apps to their iPad but must check it is appropriate for use in a school setting.
- Staff iPads are intended for the use of staff only. However, the staff member may work alongside a pupil on a staff iPad to complete a specific activity / task.
- Staff will sometimes use iPads to take photographs or video of children to celebrate a particular event, record learning or an achievement, or to publicise the work of the school (for further information, see Section - Use of digital media).
- Staff should not store their own personal photographs or data on their school iPad.
- At all times, staff should use their professional judgement and use iPads safely. If unsure, staff should seek the advice of the online Safety lead.

Management and use of pupil iPads:

- All pupil iPads are managed by the Computing co-ordinator and staff from Virtue Technologies Ltd.
- Appropriate restrictions are set so pupils cannot change the settings on an iPad or download / install apps.
- Pupils should have the permission of an adult before using an iPad.
- Pupils must only use an iPad for the activity they have obtained permission for.
- All pupil iPads connect to the schools Wifi network for internet usage. As such, they benefit from the Lancashire web filter which blocks inappropriate images and websites

USE OF MOBILE PHONES

Staff should follow the guidelines in the staff handbook pertaining to the use of personal mobile phones on the school premises.

Guests to school (including supply teachers, students and other visitors) should abide by these rules (as set out in the Acceptable Use Policy for guests – see Appendix 4).

Use of mobile phones by pupils:

- If a child brings a mobile phone to school because they walk to and from school then the phone must be given to the bursar at the start of the school day and collected from the bursar at the end of the school day.
- Pupils are not permitted to use mobile phones on the school premises. Any emergency contact can be made by staff in the school office.
- As a matter of course children should never bring into school any object or possession that is valuable (mobile phones, mp3 players, personal games consoles, portable DVD players), or an object that if they lost it, it was broken or stolen, would upset them and /or their parents.
- Children who break this rule or hide the fact that they have secreted an object into the classroom are responsible for that object themselves.
- The duty of a parent is never to allow a child bring such an object into school. The duty of a child is never to bring such an object into school or immediately inform a teacher that such an object is in their possession.
- The teacher may decide to confiscate (confiscated items should in every case be returned to a parent so that they are aware their child has brought the item into school). The item should be stored securely and safely with the bursar. This must be in a locked cabinet.

USE OF DIGITAL MEDIA (CAMERAS AND RECORDING DEVICES)
The use of cameras and sound recording devices offer substantial benefits to education and provide our school with fantastic opportunities to share experiences and memories.

PHOTOGRAPHS AND VIDEO
Photographs and videos of children are sometimes taken in school, by staff or press or parents to celebrate a particular event, record an achievement or to publicise the work of the school. These images may be used for classroom displays, school publications, newspaper articles or the school website.
As a school we follow the county guidelines regarding the use of such images, to conform with the requirements of the Data Protection Act 1998, and we therefore must seek explicit permission to take photographs or videos of children (for any purpose) if they are clearly recognisable in the photograph. The following procedures and regulations apply:
- Permission to take photographs and videos is sought in the form of a permission letter when a child starts attending our school and, if granted, lasts until they are no longer a pupil at the school (unless parents retract the permission in writing).
- If the permission letter is not returned and signed, or if a parent chooses not to give consent, staff are made aware so that photos and videos are not taken.
- Members of staff are responsible for alerting school if they do not give permission for photographs to be taken of themselves or if they do not wish their photograph to be used on the school website, in the press, in school publications or in classroom displays.
- Any member of staff has permission to take a photograph or video of any child (for the purposes outlined in the permission letter). However, photographs and videos must be taken on a school device and not on a personal device.
- Under the Data Protection Act (1998), parents are entitled to take photographs of their own children on the provision that the images are for their own use, e.g. photos taken at a school production. Parents are not to post pictures of other children on social media (unless they have the explicit permission of every parent). Parents are reminded verbally before an event of these regulations.
Storage of photographs and videos:
- All photographs and videos are stored on school devices (laptops, desktop computers and iPads), all of which are password protected.
- Staff must not store photographs of pupils on personal devices.
Publishing photographs and videos (school website):
- Photographs will only be published if the permission letter has been signed by parents.

- When a photograph or video is published (e.g. to the school website), the child's full name will not accompany it.
- The website does not provide users with an option to download images or video files from it.

USE OF COMMUNICATION TECHNOLOGIES

GOOGLE APPS FOR EDUCATION
Google Apps for Education is used to support the delivery of our curriculum in school. It was primarily designed to support remote leanring through Covid 19 school closures but will be adopted into whole school teaching as and when appropriate for the betterment of education. This system allows children to be given an email account which they can use to learn to communicate safely, responsibly and respectfully online. This email facility does allow children to send or receive email from outside the school system. Any messages sent to teachers/ staff or added to the 'stream' area of the platform will be monitored by staff and pupils must immediately report any email considered inappropriate.
As there has been an immediate need to transfer learning to remote education, many children have been introduced to this but further learning on how to use will be completed when school children back in school. As all online interactions demand, our pupils are taught how to use it safely, responsibly and respectfully.
Google meet is a visual online platform through Google Apps for education and provides the opportunity for teachers to see their pupils for the purpose of supporting teaching, learning and wellbeing. We have written a code of conduct for all parties to accompany this policy.

YOU TUBE
The school has set up a You Tube account with private settings for staff to record work safely to upload onto the school platform or use in school. Care will be taken to ensure the link is unlisted and the link would be shared through secure platforms such as Google Classrooms; email or text.

SOCIAL MEDIA / SOCIAL NETWORKS
Bretherton Endowed has a separate Social Media Policy. Please consult this for information on the use of social media by any members of our school community.
Most social media websites and applications (including Facebook) are blocked by the Lancashire Grid for Learning filtering system and cannot be used on school premises.
Bretherton uses Twitter as a social media app to inform parents of general events. Care will be taken to include only children's illustrations where our consent form permits; to not use full names and avoid any additional personal information being share.

TEACHERS TO PARENTS
Teachers to parents is used to enable school to communicate with parents via email and the mobile phone app. All personal information is stored securely within the system and is managed by the school bursar.

VIRTUAL LEARNING ENVIRONMENT (VLE): SCHOOL WEBSITE
This is available through our school website. Every pupil has a username and password which enables them to log in and communicate with others via blogs, wikis, discussions, scrapbooks or homework tasks.
Before using the VLE, pupils are taught how to use it safely, responsibly and respectfully.
This system is managed through our school website provider (School Spider Ltd) and staff members can monitor the children's use of all areas of the VLE. Any communication or comment made by a pupil that might be inappropriate (in terms of language or content) is automatically flagged up by the VLE and sent to staff for approval.

CLASS WRITING BLOGS
KS2 classes may have a writing blog (set up via 'Wordpress') and managed by class teachers. Teachers can post writing tasks / challenges as a blog post and pupils then have the ability to publish their work as a 'comment'. Pupils can also respond to each other's work using the 'reply' tool.
Before using the class writing blogs, pupils are taught how to use them safely, responsibly and respectfully.

Every comment, or reply, published by a pupil must be approved by the school e-Safety champion before it appears on the blog. This ensures that inappropriate comments are not published. Any attempt by a child to make an inappropriate comment will be taken seriously and dealt with in accordance with the school's behaviour policy.

INFRASTRUCTURE AND TECHNOLOGY

Bretherton Endowed Primary School employs the services of Virtue Technologies Ltd to manage the school's ICT infrastructure and provide regular technical assistance.

Virtue Technologies (in consultation with the Computing co-ordinator, head teacher) manage the school network, provide technical support and make appropriate recommendations.

WEB FILTERING AND VIRUS PROTECTION

Bretherton Primary School subscribes to the Lancashire Grid for Learning Broadband Service, meaning that we are provided with the Netsweeper web filtering system.

This filtering service offers a high level of protection but occasionally unsuitable content may get past the filter service. Regular updates are made so that the filter is constantly adapted to the changing online environment. Furthermore, our school has the ability to manually block additional websites or online locations which we do not want our pupils or staff to access.

Should a staff member wish to block or temporarily unblock a website, they should contact the Computing co-ordinator, deputy head teacher or head teacher.

Staff are aware that access to the internet via 3G/4G on a personal device (such as a mobile phone) means that they are not browsing using the school's broadband and, therefore, the Lightspeed web filter does not apply.

A weekly report on use of our internet service including regularly used words, blocked or concern words and possible and actual inappropriate searches. This report will be viewed by HT and ICT lead on receipt and acted upon. The results will be summarised for a termly Governor report.

Sophos Anti-Virus software is installed on all computers in school and is configured to receive regular updates automatically (via the Lancashire Grid for Learning).

SOFTWARE

- School has legal ownership of all software installed on school computers and mobile devices.
- It is the responsibility of the Computing co-ordinator (who will liaise with IT technicians from Virtue Technologies) to ensure that software is installed on devices and that licenses are kept up-to-date. This includes the installation of apps on school iPads.
- Relevant software is selected to enhance learning in all areas of the school curriculum.

4. Managing Information Systems

4.1 Maintaining Information Systems Security

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

The school broadband and online suppliers are BTLS through a Lancashire Service Level Agreement.

4.2 Password Security

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access;
- no user should be able to access another's files, without permission (or as allowed for monitoring purposes within the school's procedures);
- access to personal data is securely controlled in line with the school's personal data procedures;

A safe and secure username/password system is essential if the above is to be established and will apply to all school ICT systems, including email.

4.3 Managing Email

- Pupils may only use approved email accounts for school purposes.
- Pupils must immediately tell a designated member of staff if they receive an offensive email or one which upsets or worries them.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
- Whole-class or group email addresses will be used in primary schools for communication outside of the school.
- Staff will only use official school provided email accounts to communicate with pupils and parents, as approved by the Senior Leadership Team.
- The official school email service may be regarded as safe and secure and is monitored.
- Users need to be aware that email communications may be monitored.
- Users must immediately report, to the nominated person – in accordance with the school Policy and procedures, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and pupils or parents must be professional in tone and content.
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.
- Spam, phishing and virus attachments can make email dangerous. The school ICT provider ensures mail is virus checked (ingoing and outgoing), includes spam filtering.

4.4 Emailing Personal, Sensitive, Confidential or Classified Information

- Assess whether the information can be transmitted by other secure means before using email – emailing confidential data is not recommended and should be avoided where possible;
- Where your conclusion is that email must be used to transmit such data:

- Send the information as an encrypted document attached to an email;
- Provide the encryption key or password by a separate contact with the recipient(s);
- Do not identify such information in the subject line of any email..

- The use of EGRESS as a platform from LCC for sensitive material in relation to children, health and personal information.
- All staff and Governors to have access to @bretherton.lancs.sch.uk emails as there is a level of protection ion relation to sending communications this way through Office 365.
-

4.5 Zombie Accounts

Zombie accounts refer to accounts belonging to users who have left the school and therefore no longer have authorised access to the school's systems. User accounts will be disabled once the member of the school has left (within 4 weeks)

4.6 Managing Published Content

- The contact details on the website are the school address, email and telephone number. Staff or pupils' personal information are not published.
- The head teacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.

- The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy procedures and copyright.

4.7 Use of Digital and Video Images
- We gain parental permission for the use of digital photographs or video involving their child on our permission form.
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs.
- When using digital images, staff will inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Staff sign the school's Acceptable Use Agreement and this includes a clause on the use of mobile phones/personal equipment for taking pictures of pupils;
- Staff are allowed to take digital/video images to support educational aims, but must follow school procedures concerning the sharing, distribution and publication of those images.
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work;
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

4.8 Managing Social Networking, Social Media and Personal Publishing Sites
- The school will control access to social media and social networking sites.
- Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.
- Staff wishing to use Social Media tools with pupils as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate.
- Personal publishing will be taught via age appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.
- Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications.
- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- Newsgroups will be blocked unless a specific use is approved.
- Concerns regarding a pupil's use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents, particularly when concerning the underage use of sites.

- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and outlined in the school Staff Acceptable Use Agreement.

4.9 Managing Filtering
- The school's broadband access will include filtering appropriate to the age and maturity of pupils.
- The school will work with Netsweeper to ensure that filtering procedures are continually reviewed.
- If staff or pupils discover unsuitable sites, the URL will be reported to the School Online Safety Coordinator who will then record the incident and escalate the concern as appropriate.
- The School Senior Leadership Team will ensure that checks are made to ensure that the filtering methods selected are effective.
- Any material that the school believes is illegal will be reported to appropriate agencies such as Lancashire Police or CEOP

4.10 Managing Emerging Technologies
- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Pupils will be instructed about safe and appropriate use of personal devices both on and off site in accordance with the school Acceptable Use Agreement/Mobile Phone procedures.

4.11 Data Protection
Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:
- Fairly and lawfully processed;
- Processed for limited purposes;
- Adequate, relevant and not excessive;
- Accurate;
- Kept no longer than is necessary;
- Processed in accordance with the data subject's rights;
- Secure;
- Only transferred to others with adequate protection.

More detailed information can be found in the School Data Protection Policy.
Staff must ensure that they:
- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.

- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.

- Transfer data using encryption and secure password protected devices.

4.12 Disposal of Redundant ICT Equipment
- All redundant ICT equipment will be disposed of through an authorised agency. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
- All redundant ICT equipment that may have held personal data will have the storage media over written multiple times to ensure the data is irretrievably destroyed. Or if the storage media has failed it will be physically destroyed. We will only use authorised companies who will supply a written guarantee that this will happen.
- Disposal of any ICT equipment will conform to:

- The Waste Electrical and Electronic Equipment Regulations 2006
- The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007
- Environment Agency Guidance (WEEE) Click here to access
- ICO Guidance - Data Protection Act 1998 Click here to access
- Electricity at Work Regulations 1989

- The school will maintain a comprehensive inventory of all its ICT equipment including a record of disposal.
- The school's disposal record will include:

- Date item disposed of;
- Authorisation for disposal, including:
• verification of software licensing
• any personal data likely to be held on the storage media? *
- How it was disposed of e.g. waste, gift, sale
- Name of person and/or organisation who received the disposed item

* if personal data is likely to be held the storage media will be over written multiple times or 'scrubbed' to ensure the data is irretrievably destroyed.

E-SAFETY: ACROSS THE CURRICULUM

Bretherton Primary School provides a relevant, flexible and engaging e-Safety education to all children as part of their curriculum entitlement.

▪ As part of the Computing curriculum, e-Safety is taught explicitly in each year group (from Y1 to Y6) on an annual basis in the first half of the Spring term. During this time, Computing lessons are set aside solely for this purpose. In Key Stage 1, the topic is referred to as 'Using the internet safely'. In Key Stage 2, it is referred to as 'Working and communicating online'.

▪ To support staff in the delivery of these sessions, lesson plans and links to resources have been provided by the Computing co-ordinator. This also ensures that e-Safety teaching is progressive throughout school.

▪ Further to this, e-Safety forms a part of teaching across the entire curriculum at any time in the school year whenever technology is used to enhance learning.

▪ Safer Internet Day is celebrated annually in February and the school marks this with events throughout the day to raise awareness amongst pupils.

▪ As part of the annual anti-bullying week, children are made aware of the impact of cyberbullying and are taught how to seek help if they are affected. This is also discussed, alongside other dangers (e.g. grooming / communicating with strangers), as part of the PSHE curriculum.

▪ Children are reminded of the **e-Safety Agreement** that they have signed are given an understanding of its importance.

▪ E-Safety rules are displayed in classrooms so that pupils are reminded of safe internet use.

▪ Children are taught that e-Safety applies to their lives outside school (not just their work inside school).

5. Policy Decisions

5.1 Authorising Internet Access

- All staff will read and sign the Staff Acceptable Use Agreement before using any school ICT resources.
- Parents will be asked to read and sign the School Acceptable Use Agreement for pupil access and discuss it with their child, where appropriate.

- At Key Stage 1, pupils' access to the Internet will be by adult demonstration with occasional directly supervised access to specific and approved online materials.
- At Key Stage 2, pupils will be supervised. Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary.

5.2 Assessing Risks
- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor the LA can accept liability for the material accessed, or any consequences resulting from Internet use.
- The school will audit ICT use to establish if the Online Safety Policy and procedures is adequate and that the implementation of the Online Safety Policy is appropriate – see Appendix A for a sample Online Safety Audit.

5.3 Unsuitable/Inappropriate Activities
The school believes that the activities referred to in the following section would be inappropriate in a school context and users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school Policy and procedures restricts certain internet usage as follows:

This table sets out typical procedures and sanctions for possible incidents:

Incident	Procedure and Sanctions
<u>Accidental</u> access to inappropriate materials.	▪ Minimise the webpage/turn the monitor off. ▪ Tell a trusted adult. ▪ Enter the details in the Incident Log and report to LGfL filtering services if necessary. ▪ Persistent 'accidental' offences may result in further disciplinary action in line with the behaviour policy.
Using other people's logins and passwords maliciously. Deliberate searching for inappropriate materials. Bringing inappropriate electronic files from home. Using chats and forums in an inappropriate way.	▪ Inform the eSafety Champion / a member of the SLT team. ▪ Enter the details in the Incident Log. ▪ Additional awareness raising of eSafety issues and the AUP with individual child/class. ▪ More serious or persistent offences may result in further disciplinary action in line with Behaviour Policy. ▪ Consider parent/carer involvement.

when using school equipment or systems. The school Policy and procedures restricts certain internet usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	child sexual abuse images					✓
	promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation					✓
	adult material that potentially breaches the Obscene Publications Act in the UK					✓
	criminally racist material in UK					✓
	pornography				✓	
	promotion of any kind of discrimination				✓	
	promotion of racial or religious hatred				✓	
	threatening behaviour, including promotion of physical violence or mental harm				✓	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				✓	
Using school systems to run a private business					✓	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					✓	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					✓	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer / network access codes and passwords)					✓	
Creating or propagating computer viruses or other harmful files					✓	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet					✓	

Version No: 1
Last Review Date: March 2017

User Actions	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and Illegal
Online gaming (educational)		✓			
Online gaming (non-educational)				✓	
Online gambling				✓	
Online shopping/commerce			✓		
File sharing				✓	
Use of social networking sites				✓	
Use of video broadcasting e.g. Youtube			✓		

School will deal with incidents of inappropriate use quickly and in line with both the e-Safety policy and the school's behaviour policy.
This table sets out typical procedures and sanctions for possible incidents:

Incident Procedure and Sanctions

Accidental access to inappropriate materials.

Using other people's logins and passwords maliciously.

- Minimise the webpage/turn the monitor off.
- Tell a trusted adult.
- Enter the details in the Incident Log and report to LGfL filtering services if necessary.
- Persistent 'accidental' offences may result in further disciplinary action in line with the behaviour policy.

Deliberate searching for inappropriate materials.
Bringing inappropriate electronic files from home.
Using chats and forums in an inappropriate way.

- Inform the eSafety lead/ a member of the SLT team.
- Enter the details in the Incident Log.
- Additional awareness raising of eSafety issues and the AUP with individual child/class.
- More serious or persistent offences may result in further disciplinary action in line with Behaviour Policy.
- Consider parent/carer involvement.

5.4 What are the risks?

The risks that can be posed to young people and adults when online have been identified by the EUKids online project, which was later referenced in paragraph 1.3 of Dr Tanya Byron in "Safer Children in a Digital World" (2008).

	Commercial	Aggressive	Sexual	Values
Content (Child as recipient)	Adbert Spam Sponsorship Personal info	Violent/ hateful content	Pornographic or unwelcome sexual content	Bias Racist or misleading info or advice
Contact (Child as participant)	Tracking Harbesting Personal info	Being bullied Harassed or stalked	Meeting strangers Being grooed	Self harm Unwelcome persuasions
Conduct (Child as actor)	Illegal downloading Hacking Gambling Financial scams Terrorism	Bullying or harassing another	Creating and uploading inappropriate material	Providing misleading information. advice

5.5 Responding to Incidents of Concern

If any apparent or actual misuse appears to involve illegal activity e.g.

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- extremism or radicalisation of individuals
- other criminal conduct, activity or materials

- school should refer to the Flow Chart found at Appendix I.

- The Online Safety Coordinator will record all reported incidents and actions taken in the School Online Safety incident log and other in any relevant areas e.g. Bullying or Child protection log.
- The Designated Safeguarding Lead will be informed of any online safety incidents involving Child Protection concerns, which will then be escalated appropriately – See Child Protection Policy and procedures for dealing with concerns.
- The school will manage Online Safety incidents in accordance with the school discipline/behaviour policy where appropriate.
- The school will inform parents of any incidents of concerns as and when required.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Safeguarding Hub **and** escalate the concern to the Police.
- If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Safeguarding Hub – see Child Protection Policy and procedures.

5.6 Managing Cyber-bullying

- Cyber-bullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the Whole School Behaviour Policy.
- There are clear procedures in place to support anyone in the school community affected by cyber-bullying.
- All incidents of cyber-bullying reported to the school will be recorded.
- There will be clear procedures in place to investigate incidents or allegations of Cyber-bullying.

5.7 Managing Mobile Phones and Personal Devices

The use of mobile phones and other personal devices by pupils is not allowed. If a child brings a personal mobile phone for walking to and from school, this will be handed into the school office at the start of day and collected at the end.

Pupils use of personal devices:
- If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents/carers in accordance with the school policy.
- If a pupil needs to contact his/her parents/carers they will be allowed to use a school phone.

Staff use of personal devices:
- Mobile phones and communication devices should be switched off or switched to 'silent' mode. Bluetooth communication should be "hidden" or switched off.
- Mobile phones of staff must be stored out of sight and not used in the proximity of children, eg. in the classroom.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose.
- Where members of staff are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting pupils or parents, then a school mobile phone will be provided and used. In an emergency where a staff member does not have access to a school-owned device, they should use their own device.
- If a member of staff breaches the school Policy and procedures then disciplinary action may be taken.

6. Communicating Policy and procedures

6.1 Introducing the Policy and procedures to Pupils

• All users will be informed that network and Internet use will be monitored.

• An online safety training programme will be established across the school to raise the awareness and importance of safe and responsible internet use amongst pupils.

• Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.

6.2 Discussing the Policy and procedures with Staff

- The Online Safety Policy and procedures will be formally provided to, and discussed, with all members of staff.
- To protect all staff and pupils, the school will implement Acceptable Use Agreements.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.

6.3 Enlisting Parents' Support

- Parents' attention will be drawn to the school Online Safety Policy and procedures in newsletters, and on the school website.

- A partnership approach to online safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use, or highlighting online safety at other attended events.
- Parents will be encouraged to read and sign the school Acceptable Use Agreement for pupils and discuss its implications with their children.
- Information and guidance for parents on online safety will be made available to parents in a variety of formats.
- In the event of online safety concerns for a child at home (not evidenced in school), parents will be contacted at first incident by IT lead or SLT to investigate the validity and impact and seek to support a resolve of the situation. If a child is exposed to inappropriate online content or is indicated to be breaching our anti bullying policy, a meeting will be called by school with the parents and child to see a resolution.

7. Complaints

The school will take all reasonable precautions to ensure online safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable materials will never appear on a school computer or mobile device. Neither the school staff nor the Governing Body can accept liability for material accessed, or any consequences of Internet access.

- Complaints about the misuse of on-line systems will be dealt with under the school's Complaints procedure.
- Complaints about cyberbullying are dealt with in accordance with our Anti-bullying procedures.
- Complaints related to child protection are dealt with in accordance with school/LA Child Protection Policy and procedures.
- Any complaints about staff misuse will be referred to the Head teacher.
- All online safety complaints and incidents will be recorded by the school including any actions taken (see Appendix J).

Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

- Interview/counselling by class teacher/Online Safety Coordinator/Head teacher;
- Informing parents;
- Removal of Internet or computer access for a period, which could ultimately prevent access to files held on the system, including examination coursework);
- Referral to the Police.

Our Online Safety Coordinator acts as the first point of contact for any complaint. Any complaint about staff misuse is referred to the Head teacher.

Appendix A

Bretherton Endowed CE Primary school ONLINE SAFETY AUDIT

This self-audit should be completed by the member of the Senior Leadership Team (SLT) responsible for Online Safety.

Date of latest update: September 2019
Date of future review: September 2021
The school Online Safety Policy and procedures was agreed by governors on: September 2019
The Policy and procedures is available for staff to access at: staff room board
The Policy and procedures is available for parents to access at: www.brethertonschool.org.uk

The Governor responsible for Online Safety is: Laurence Glew
The Designated Safeguarding Lead is: Alison Moxham
The Online Safety Coordinator is: Sarah Allchurch

Were all stakeholders (e.g. pupils, staff and parents) consulted when updating the school Online Safety Policy and procedures?	**YES / NO**
Has up-to-date Online Safety training been provided for all members of staff? (not just teaching staff)	**YES / NO**
Do all members of staff sign an Acceptable Use Agreement on appointment?	**YES / NO**
Are all staff made aware of the schools expectation around safe and professional online behaviour?	**YES / NO**
Is there a clear procedure for staff, pupils and parents to follow when responding to or reporting an online safety incident of concern?	**YES / NO**
Have online safety materials from CEOP, Childnet and UKCCIS etc. been obtained?	**YES / NO**
Is online safety training provided for all pupils (appropriate to age and ability and across all Key Stages and curriculum areas)?	**YES / NO**
Are online safety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all pupils?	**YES / NO**
Do parents or pupils sign an Acceptable Use Agreement?	**YES / NO**
Are staff, pupils, parents and visitors aware that network and Internet use is closely monitored and individual usage can be traced?	**YES / NO**

Has an ICT security audit been initiated by SLT? **YES / NO**

Is personal data collected, stored and used according to the principles of the Data Protection Act? **YES / NO**

Is Internet access provided by an approved educational Internet service provider which complies with DfE requirements? **YES / NO**

Has the school filtering been designed to reflect educational objectives and been approved by SLT? **YES / NO**

Are members of staff with responsibility for managing filtering, network access and monitoring systems adequately supervised by a member of SLT? **YES / NO**

Does the school log and record all online safety incidents, including any action taken? **YES / NO**

Are the Governing Body and SLT monitoring and evaluating the school Online Safety Policy and procedures on a regular basis? **YES / NO**

Appendix B

KS1 E-SAFETY RULES

Our Rules for Staying Safe with ICT

We only use the Internet when a trusted adult is with us.

We are always polite and friendly when using online tools.

We always make careful choices when we use the internet.

We always ask a trusted adult if we need help using the Internet.

We always tell a trusted adult if we find something that upsets us.

KS2 E-SAFETY RULES

Our Rules for Staying Safe with ICT

We always ask permission before using the internet.

We only use the Internet when a trusted adult is around.

We immediately close/minimise any page we are uncomfortable with (or if possible switch off the monitor / iPad screen).

We always tell an adult if we see anything we are uncomfortable with.

We only communicate online with people a trusted adult has approved.

All our online communications are polite and friendly.

We never give out our own, or others', personal information or passwords and are very careful with the information that we

share online.

We only use programmes and content which have been installed by the school.

Appendix C   -   EYFS, Primary & Special School Pupil Acceptable Use Agreement

Primary Pupil Acceptable Use

Bretherton Endowed Primary School
Agreement / E- Safety Rules

- I will only use ICT 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 ICT passwords

- I will only open/delete my own files

- I will make sure that all ICT 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/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 ICT because I know that these rules are to keep me safe

- I will support the school approach to online safety and not upload or add any images, video, sounds or text that could upset any member of the school community

- I know that my use of ICT can be checked and my parent/carer contacted if a member of school staff is concerned about my safety

- I will not sign up for any online service unless this is an agreed part of a school project approved by my teacher

- I will not bring a Smart Watch to school because I am not allowed to wear one during the school day

- I will not sign up to online services until I am old enough

Dear Parent/ Carer

ICT including the internet, email and mobile technologies has become an important part of learning in our school.   We expect all children to be safe and responsible when using any ICT.

Please read and discuss these E-Safety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact the school office on 01772 614300

Please take care to ensure that appropriate systems are in place at home to protect and support your child/ren.

✂ -

Parent/ carer signature
We have discussed this document with…………………………….........(child's name)
and we agree to follow the E-Safety rules and to support the safe use of ICT at Bretherton Endowed School.

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

Class ……………………………… Date ………………………………

Appendix D   -   Staff/Volunteer Acceptable Use Agreement

> # ICT Acceptable Use Policy (AUP) – Staff and Governors

ICT and the related technologies such as e-mail, the Internet and mobile devices are an integral part of our daily life in school. This agreement is designed to ensure that all staff and Governors are aware of their individual responsibilities when using technology. All staff members and Governors are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the head teacher.

1. I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.

2. I will be an active participant in e-Safety education, taking personal responsibility for my awareness of the opportunities and risks posed by the use of technology.

3. I will not use communications devices, whether school provided or personally owned, for bullying or harassment of others in any form.

4. I will not be involved with any online activities, either within or outside school that may bring the school, staff, children or wider members into disrepute. This includes derogatory/inflammatory comments made on Social Network Sites, Forums and Chat rooms.

5. I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory.

6. I will respect copyright and intellectual property rights.

7. I will ensure that all electronic communications with children and other adults are appropriate.

8. I will not use the school system(s) for personal use during working hours.

9. I will not install any hardware or software without the prior permission of the head teacher, deputy head teacher or computing coordinator.

10. I will ensure that personal data (including data held on MIS systems) is kept secure at all times and is used appropriately in accordance with Data Protection legislation.

11. I will ensure that images of children and/or adults will be taken, stored and used for professional purposes in line with school policy and with written consent of the parent/carer or relevant adult. I will not distribute images outside the school network
without the prior permission of the parent/carer, or person/s in the image.

12. I will abide by the school's rules for using personal mobile equipment, including my mobile phone, at all times.

13. I will report any known misuses of technology, including the unacceptable behaviours of others.

14. I have a duty to respect the technical safeguards which are in place. I understand that attempting to breach technical safeguards or gain unauthorised access to systems and services is unacceptable.

15. I have a duty to report failings in technical safeguards which may become apparent when using the systems and services.

16. I have a duty to protect passwords and personal network logins, and should log off the network when leaving workstations unattended. I understand that any attempts to access,
corrupt or destroy other users' data, or compromise the privacy of others in any way, using any technology, is unacceptable.

17. I understand that network activities and online communications are monitored, including any personal and private communications made using school systems.

18. I am aware that in certain circumstances where unacceptable use is suspected, enhanced monitoring and procedures may come into action, including the power to confiscate personal technologies such as mobile phones.

19. I will take responsibility for reading and upholding the standards laid out in the AUP. I will support and promote the school's e-Safety policy and help children to be safe and responsible in their use of ICT and related technologies.

20. I understand that these rules are designed for the safety of all users and that if they are not followed, school sanctions will be applied and disciplinary action taken.

21. In the event of remote learning, I will apply the same concern for children's safety as face to face and look for ways to minimise any risks to inappropriate content when setting lessons online.

22. I understand the need to keep the children and myself safe when conducting online visual meetings (for example through Covid 19 remote learning) and will follow the school's guidance and code of conduct and at ant time, I do not feel this is happening, I will cancel the meet and inform SLT at the earliest convenience.

23. If working 1 to 1 on the visual online plaform (Google meet), I will request an adult is in the vicinity of the child on the computer or advise that the session will be recorded.

User Signature

I have read and agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature …………………………………………..…………………………………………………………..

Date ………..

Full Name ………………………………………………………………………………..………… (PRINT)

Position/Role …………………………………………………………………………………………………….

ICT Acceptable Use Policy (AUP) – Visitors

To be signed by any adult working in the school for a short period of time.
This includes student teachers, supply teachers, volunteers, visitors, etc.

1. I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.
2. I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory.
3. I will not use any external device to access the school's network e.g. pen drive.
4. I will respect copyright and intellectual property rights.
5. I will ensure that images of children and/or adults will be taken, stored and used for professional purposes in line with school policy and with written consent of the parent/carer or relevant adult. I will not distribute images outside the school network without the prior permission of the parent/carer, or person/s in the image.
6. I will abide by the school's rules for using personal mobile equipment, including my mobile phone, at all times.
7. I understand that network activities and online communications are monitored, including any personal and private communications made using school systems.
8. I will not install any hardware or software onto any school system.
9. I understand that these rules are designed for the safety of all users and that if they are not followed, school sanctions will be applied and disciplinary action taken.

User Signature

I have read and agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature …….
Date ……..
Full Name ……………………………………………………………………………………………………… (PRINT)
Position/Role ……………………………………………………………………………………………………….

Appendix E   -   Social Networking Sites (Facebook) Guidance for Parents

SOCIAL NETWORKING SITES - FACEBOOK
GUIDANCE FOR PARENTS

There are many children of Primary School age who have Facebook Profiles despite the permitted minimum age to use the site being 13, according to the site terms and conditions.

Our school is committed to promoting the safe and responsible use of the Internet and as such we feel it is our responsibility to raise this particular issue as a concern. Whilst children cannot access Facebook or other social networking sites at school, they could have access to it on any other computer or mobile technology. Websites such as Facebook offer amazing communication and social connections, however they are created with their audience in mind and this is specifically 13 years old. Possible risks for children under 13 using the site may include:

- Facebook use 'age targeted' advertising and therefore your child could be exposed to adverts of a sexual or other inappropriate nature, depending on the age they stated they were when they registered;
- Children may accept 'friend requests' from people they don't know in real life which could increase the risk of inappropriate contact or behaviour;
- Facebook is one of the social networking sites used by those attempting to radicalise young people;
- Language, games, groups and content posted or shared on Facebook is not moderated, and therefore can be offensive, illegal or unsuitable for children;
- Photographs shared by users are not moderated and therefore children could be exposed to inappropriate images or even post their own;
- Underage users might be less likely to keep their identities private and lying about their age can expose them to further risks regarding privacy settings and other options;
- Facebook could be exploited by bullies and for other inappropriate contact;
- Facebook cannot and does not verify its members therefore it important to remember that if your child can lie about who they are online, so can anyone else!

We feel that it is important to point out to parents the risks of underage use of such sites, so you can make an informed decision as to whether to allow your child to have a profile or not. These profiles will have been created away from school and sometimes by a child, their friends, siblings or even parents. We will take action (such as reporting aged profiles) if a problem comes to our attention that involves the safety or wellbeing of any of our children.

Should you decide to allow your children to have a Facebook profile we strongly advise you to:
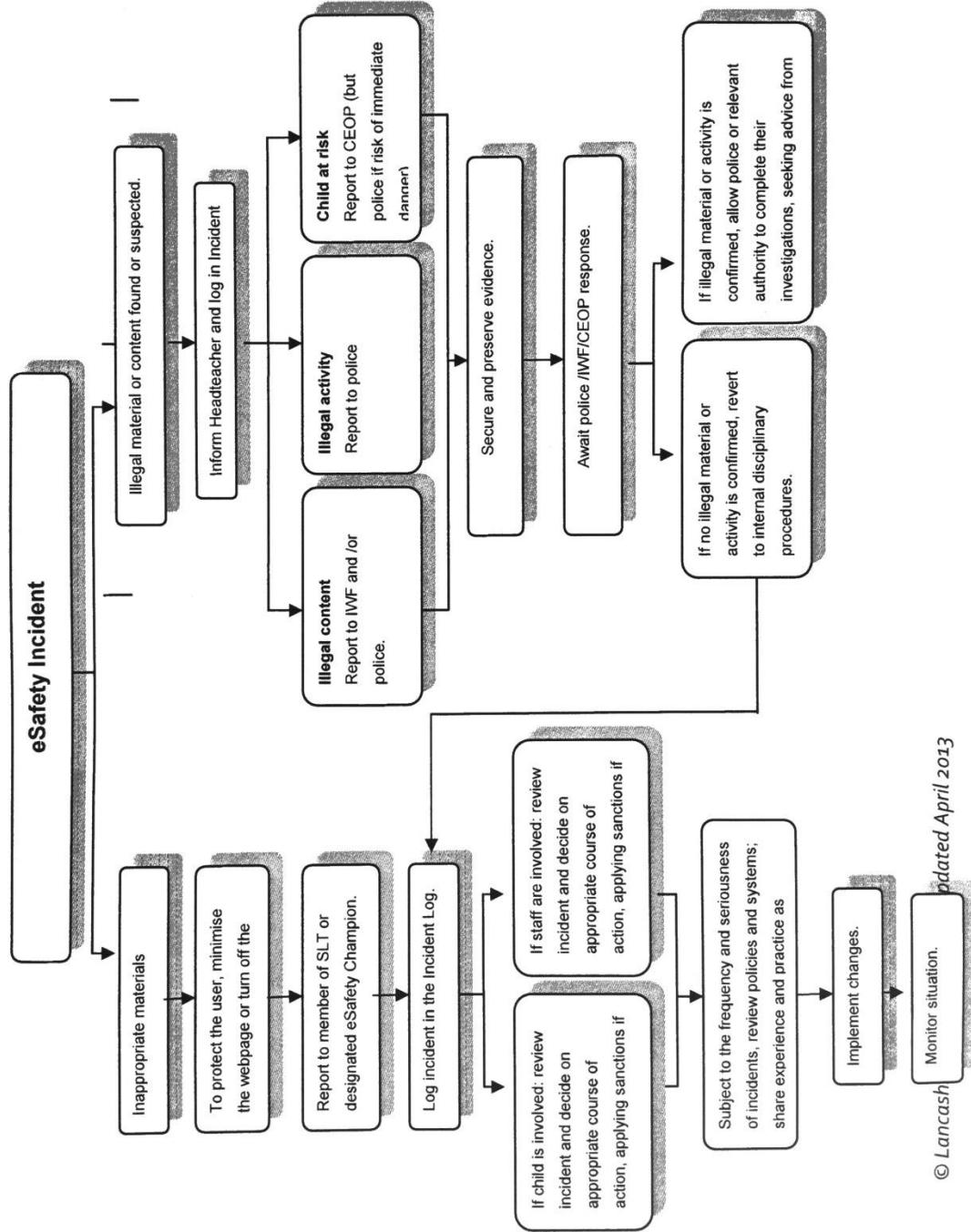
- Check their profile is set to private and that only 'friends' can see information that is posted;
- Monitor your child's use and talk to them about safe and appropriate online behaviour such as not sharing personal information and not posting offensive messages or photos;
- Ask them to install the CEOP (Child Exploitation and Online Protection Centre) application from www.facebook.com/clickceop on their profile. This places a bookmark on their profile to CEOP and the 'Report Abuse' button which has been known to deter offenders;
- Have a look at the advice for parents from Facebook www.facebook.com/help/?safety=parents;
- Set up your own profile so you understand how the site works and ask them to add you as a friend on their profile so you can keep track of what they are posting online;
- Make sure your child understands the following rules:

➢ Always keep your profile private;
➢ Never accept friends you don't know in real life;
➢ Never post anything which could reveal your identity;
➢ Never post anything you wouldn't want your parents to see;

➢ Never agree to meet someone you only know online without telling a trusted adult;
➢ Always tell someone if you feel threatened or someone upsets you.

We recommend that all parents visit the CEOP ThinkUKnow website for more information on keeping your child safe online

Appendix F   -   Response to an Incident or Concern Flow Chart

Responding to eSafety Incident/ Escalation Procedures

eSafety Incident

Illegal material or content found or suspected.

Inform Headteacher and log in Incident

Illegal content
Report to IWF and /or police.

Illegal activity
Report to police

Child at risk
Report to CEOP (but police if risk of immediate danger)

Secure and preserve evidence.

Await police /IWF/CEOP response.

If illegal material or activity is confirmed, allow police or relevant authority to complete their investigations, seeking advice from

If no illegal material or activity is confirmed, revert to internal disciplinary procedures.

Inappropriate materials

To protect the user, minimise the webpage or turn off the

Report to member of SLT or designated eSafety Champion.

Log incident in the Incident Log.

If child is involved: review incident and decide on appropriate course of action, applying sanctions if

If staff are involved: review incident and decide on appropriate course of action, applying sanctions if

Subject to the frequency and seriousness of incidents, review policies and systems; share experience and practice as

Implement changes.

Monitor situation.

© Lancash   *Updated April 2013*

Appendix G   -   Sample Online Safety Incident Log

Bretherton Endowed CE Primary School
Details of Online Safety incidents to be recorded by the Online Safety Coordinator. This incident log will be monitored termly by the Head teacher and the Resources and Finance sub-committee of the governing body.

Date	Time	Name of Pupil or Staff Member	Male or Female	Room and Computer/ Device No.	Details of Incident (including Evidence)	Actions and Reasons

Appendix H   -   Online Safety Links

The following links may help those who are developing or reviewing a school Online Safety Policy and procedures.

 CEOP (Child Exploitation and Online Protection Centre):

 Childline:

 Childnet:

 Internet Watch Foundation (IWF):

 Cumbria Local Safeguarding Children Board (Cumbria LSCB):

 Kidsmart:

 Think U Know website:

 Virtual Global Taskforce — Report Abuse:

 EE Safety Education:

 O2 Safety Education:

 Information Commissioner's Office (ICO)

 INSAFE

 Anti-Bullying Network -

 Cyberbullying.org -

 Learning Curve Education:

 UK Safer Internet Centre:

 UK Council for Child Internet Safety (UKCCIS):

 Wise Kids:

 Teem:

 Know the Net:

 Family Online Safety Institute:

 e-safe Education:

 Facebook Advice to Parents:

 Test your online safety skills:

The above internet site links were correct at the time of publishing. School staff are advised to check the content of each site prior to allowing access to pupils.

Department for Education/Home Office guidance for schools

PREVENT Duty statutory guidance for Public Bodies: England and Wales – March 2015

The PREVENT Duty – non-statutory Departmental advice for Schools and Childcare Providers – DfE – June 2015

How Social Media is used to encourage travel to Syria and Iraq – Home Office advice to schools – June 2015

Appendix I - **Legal Framework**

LEGAL FRAMEWORK

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Criminal Justice Act 2003

Section 146 of the Criminal Justice Act 2003 came into effect in April 2005, empowering courts to impose tougher sentences for offences motivated or aggravated by the victim's sexual orientation in England and Wales.

Sexual Offences Act 2003

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). This can include images taken by and distributed by the child themselves (often referred to as "Sexting"). A person convicted of such an offence may face up to 10 years in prison.

The offence of grooming is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence.

Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification.

It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff etc. fall in this category of trust).

Any sexual intercourse with a child under the age of 13 commits the offence of rape.

N.B. Schools should have a copy of The Home Office "Children & Families: Safer from Sexual Crime" document as part of their child protection packs. Click here to access.

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Data Protection Act 1998

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

• Fairly and lawfully processed

• Processed for limited purposes

• Adequate, relevant and not excessive

• Accurate

• Not kept longer than necessary

• Processed in accordance with the data subject's rights

• Secure
 • Not transferred to other countries without adequate protection

The Computer Misuse Act 1990 (sections 1 - 3)
This Act makes it an offence to:
• Erase or amend data or programs without authority;
• Obtain unauthorised access to a computer;
• "Eavesdrop" on a computer;
• Make unauthorised use of computer time or facilities;
• Maliciously corrupt or erase data or programs;
• Deny access to authorised users.

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)
This legislation makes it a criminal offence to send an electronic message (email) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988
Copyright is the right to prevent others from copying or using his or her "work" without permission. The material to which copyright may attach (known in the business as "work") must be the author's own creation and the result of some skill and judgement. It comes about when an individual expresses an idea in a tangible form. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer.
It is an infringement of copyright to copy all or a substantial part of anyone's work without obtaining the author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Trade Marks Act 1994
This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Public Order Act 1986 (sections 17 — 29)
This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Obscene Publications Act 1959 and 1964
Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997
A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Freedom of Information Act 2000
The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Regulation of Investigatory Powers Act 2000
It is an offence for any person to intentionally and without lawful authority intercept any communication.
Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.
- Criminal Justice and Immigration Act 2008
- Section 63 offence to possess "extreme pornographic image"
- 63 (6) must be "grossly offensive, disgusting or otherwise obscene"
- 63 (7) this includes images of "threats to a person life or injury to anus, breasts or genitals, sexual acts with a corpse or animal whether alive or dead" must also be "explicit and realistic". Penalties can be up to 3 years imprisonment.
- Education and Inspections Act 2006
- Education and Inspections Act 2006 outlines legal powers for schools which relate to Cyber-bullying/ Bullying:
- • Head teachers have the power "to such an extent as is reasonable" to regulate the conduct of pupils off site.
- • School staff are able to confiscate items such as mobile phones etc. when they are being used to cause a disturbance in class or otherwise contravene the school behaviour/anti-bullying procedures.
- Telecommunications Act 1984
- It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.
- Criminal Justice & Public Order Act 1994
- This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:
- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.
- Human Rights Act 1998
- This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the school context, human rights to be aware of include:
- The right to a fair trial.
- The right to respect for private and family life, home and correspondence.
- Freedom of thought, conscience and religion.
- Freedom of expression.
- Freedom of assembly.
- Prohibition of discrimination.
- The right to education.

- These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

Appendix J

GLOSSARY OF TERMS

Becta British Educational Communications and Technology Agency (Government agency promoting the use of information and communications technology) – *NOTE: Becta Closed in 2011*

CEOP Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.

CLEO The Regional Broadband Consortium of Cumbria and Lancashire – is the provider of broadband and other services for schools and other organisations in Cumbria and Lancashire

CPD Continuous Professional Development

DfE Department for Education

FOSI Family Online Safety Institute

HSTF Home Secretary's Task Force on Child Protection on the Internet

ICO Information Commissioners Office

ICT Information and Communications Technology

ICTMark Quality standard for schools provided by Naace Click here to access

INSET In Service Education and Training

IP address The label that identifies each computer to other computers using the IP (internet protocol)

ISP Internet Service Provider

ISPA Internet Service Providers' Association

IWF Internet Watch Foundation

JANET Provides the broadband backbone structure for Higher Education and for the National Education Network.

KS1 Key Stage 1 (2, 3, 4 or 5) – schools are structured within these multiple age groups e.g. KS3 = years 7 to 9 (age 11 to 14)

LA Local Authority

LAN Local Area Network

Learning A learning platform brings together hardware, software and supporting services to support
Platform teaching, learning, management and administration.

LSCB Local Safeguarding Children Board

MIS Management Information System

MLE Managed Learning Environment

NEN National Education Network – works with the Regional Broadband Consortia (e.g. CLEO in Cumbria) to provide the safe broadband provision to schools across Britain.

Ofcom Office of Communications (Independent communications sector regulator)

Ofsted Office for Standards in Education, Children's Services and Skills

PDA Personal Digital Assistant (handheld device)

PHSE Personal, Health and Social Education

RBC Regional Broadband Consortia (e.g. CLEO) have been established to procure broadband connectivity for schools in England. There are 13 RBCs covering most local authorities in England, Wales and Northern Ireland.

SEF Self Evaluation Form – used by schools for self-evaluation and reviewed by Ofsted prior to visiting schools for an inspection

TUK Think U Know – educational E-Safety programmes for schools, young people and parents.

URL Uniform Resource Locator (URL) it is the global address of documents and other resources on the World Wide Web.

VLE Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,

WAP Wireless Application Protocol

Appendix K

Advice for Children on Cyber-bullying

If you're being bullied by phone or the Internet

- Remember, bullying is never your fault. It can be stopped and it can usually be traced.

- Don't ignore the bullying. Tell someone you trust, such as a teacher or parent, or call an advice line.

- Try to keep calm. If you are frightened, try to show it as little as possible. Don't get angry, it will only make the person bullying you more likely to continue.

- Don't give out your personal details online - if you're in a chatroom, watch what you say about where you live, the school you go to, your email address etc. All these things can help someone who wants to harm you build up a picture about you.

- Keep and save any bullying emails, text messages or images. Then you can show them to a parent or teacher as evidence.

- If you can, make a note of the time and date bullying messages or images were sent, and note any details about the sender.

There's plenty of online advice on how to react to cyberbullying. For example, www.kidscape.org and www.wiredsafety.org have some useful tips:

Text/video messaging
You can easily stop receiving text messages for a while by turning off incoming messages for a couple of days. This might stop the person texting you by making them believe you've changed your phone number. To find out how to do this, visit www.wiredsafety.org.
- If the bullying persists, you can change your phone number. Ask your mobile service provider
- Don't reply to abusive or worrying text or video messages. Your mobile service provider will have a number for you to ring or text to report phone bullying. Visit their website for details.
- Don't delete messages from cyberbullies. You don't have to read them, but you should keep them as evidence.

Text harassment is a crime. If the calls are simply annoying, tell a teacher, parent or carer. If they are threatening or malicious and they persist, report them to the police, taking with you all the messages you've received.

Phone calls
- If you get an abusive or silent phone call, don't hang up immediately. Instead, put the phone down and walk away for a few minutes. Then hang up or turn your phone off. Once they realise they can't get you rattled, callers usually get bored and stop bothering you.

- Don't give out personal details such as your phone number to just anyone. And never leave your phone lying around. When you answer your phone, just say 'hello', not your name. If they ask you to confirm your phone number, ask what number they want and then tell them if they've got the right number or not.
- You can use your voicemail to vet your calls. A lot of mobiles display the caller's number. See if you recognise it. If you don't, let it divert to voicemail instead of answering it.
- And do not leave your name on your voicemail greeting. You could get an adult to record your greeting. Their voice might stop the caller ringing again. Almost all calls nowadays can be traced.
- If the problem continues, think about changing your phone number.
- If you receive calls that scare or trouble you, make a note of the times and dates and report them to the police. If your mobile can record calls, take the recording too.

Emails
- Never reply to unpleasant or unwanted emails — the sender wants a response, so don't give them that satisfaction.
- Keep the emails as evidence. And tell an adult about them.
- Ask an adult to contact the sender's Internet Service Provider (ISP) by writing abuse@ and then the host, e.g. abuse@hotmail.com
- Never reply to someone you don't know, even if there's an option to 'unsubscribe'. Replying simply confirms your email address as a real one.

Web bullying
- If the bullying is on a website (e.g. Bebo) tell a teacher or parent, just as you would if the bullying was face-to-face – even if you don't actually know the bully's identity. Serious bullying should be reported to the police - for example threats of a physical or sexual nature. Your parent or teacher will help you do this.

Chat rooms and instant messaging
- Never give out your name, address, phone number, school name or password online.
- It's a good idea to use a nickname. And don't give out photos of yourself.
- Don't accept emails or open files from people you don't know. Remember it might not just be people your own age in a chatroom.
- Stick to public areas in chat rooms and get out if you feel uncomfortable.
- Tell your parents or carers if you feel uncomfortable or worried about anything that happens in a chat room.
- Think carefully about what you write; don't leave yourself open to bullying.
- Don't ever give out passwords to your mobile or email account.
- Three steps to stay out of harm's way
- Respect other people - online and off. Don't spread rumours about people or share their secrets, including their phone numbers and passwords.
- If someone insults you online or by phone, stay calm – and ignore them.
- Think how you would feel if you were bullied. You're responsible for your own behaviour – make sure you don't distress other people or cause them to be bullied by someone else.

Appendix L – Parent consent form

Appendix M – e safety agreement

Adopted : September 2019

To be reviewed :No later than 2021

All aspects of our policy intends to comply within the Data Protection (GDPR) legislation.

Headteacher : Mrs Alison Moxham   Chair of Governors : Mr T. G. Wilson   www.brethertonschool.org.uk