St Herbert's CE (VA) Primary & Nursery School

ONLINE SAFETY POLICY & PROCEDURE

Spring 2022

Contents

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

Note: Not all of the Appendices will be appropriate or deemed necessary for your school and only those required/ approved should be used with your Policy and procedures. Please ensure that all statements within the Acceptable Use Agreements are appropriate and necessary for your setting

POLICY

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.

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:

- Overarching Safeguarding Statement
- Child Protection Policy and procedures
- Data Protection Policy
- Health and Safety Policy and procedures
- Whole School Behaviour Policy
- Procedures for Using Pupils' Images
- Code of Conduct for staff and other adults
- Voluntary Home-School Agreement

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//staffroom/shared staff drive
- Policy and procedures to be discussed as part of the school induction pack for new staff and other relevant adults including (where relevant) the staff Acceptable Use Agreement
- Acceptable Use Agreements discussed with pupils at the start of each year
- Acceptable Use Agreements to be issued to external users of the school systems (e.g. Governors) usually on entry to the school
- 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.

The review period for this Policy and procedures is as determined by the Governing Body/Proprietors and indicated on the front cover.

4. Schedule for Development / Monitoring / Review

This Online Safety Policy and procedures was approved by the *Governing Body/Governing Body Committee on:*	Spring 2022
The implementation of this Online Safety Policy and procedures will be monitored by the:	*S. Hughes (Headteacher)* *A.Mann(Computing/online safety Leader in School)* *C.Hope (Chair of Governors)*
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:	*Annually*
Should serious Online safety incidents take place, the following external persons/agencies will be informed:	*LA ICT Manager, DO, Police, Information Commissioner's Office*

The school will monitor the impact of the Policy and procedures using:

- *Logs of reported incidents*

- *Internal monitoring data for network activity*
- *Surveys/questionnaires of*
    - *pupils (e.g. Ofsted "Tell-us" survey/CEOP ThinkUknow survey)*
    - *parents*
    - *staff*

5. 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 our 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 & online safety Governor 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. A member of the Governing Body has taken on the role of Online Safety Governor.
- support the school in encouraging parents and the wider community to become engaged in online safety activities.
- regular review with the Online Safety Coordinator (including incident logs)and incorporate any online safety into standing discussions of safeguarding at governors meetings.
- 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 and making use of the document from the UK Council for Internet Safety (UKCIS) Online safety in schools and colleges: Questions from the Governing Board .
- ensure that as the online safety coordinator is not the named DSL or deputy DSL, there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised.
- check that Annex C - Online Safety which forms part of 'Keeping Children Safe in Education' reflects practice in the school.
- ensure that all staff undertake safeguarding and child protection training (including online safety) at induction which is regularly updated in line with advice from the Local Safeguarding Children Partnership (SCP).
- ensure that appropriate filters and appropriate monitoring systems are in place. Consideration should be given to 'over-blocking' which may lead to unreasonable restrictions as to what pupils can be taught in relation to online teaching and safeguarding.
- ensure pupils are taught how to keep themselves safe, including online as part of providing a broad and balanced curriculum with clear procedures on the use of mobile technology.

1.2 Head teacher

The Head teacher has overall responsibility for online safety provision. The day-to-day responsibility for online safety may be delegated to the Online Safety Coordinator/Designated Safeguarding Lead (DSL).

The Head teacher will:

- take overall responsibility for data and data security;
- foster a culture of safeguarding where online safety is fully integrated into whole school safeguarding;
- oversee the activities of the DSL and ensure that the DSL responsibilities listed in the section below are being followed and fully supported;
- ensure that Policies and procedures are followed by all staff;
- undertake training in offline and online safety, in accordance with statutory guidance and relevant Local Safeguarding Partnership recommendations;
- liaise with the designated safeguarding lead on all online-safety issues which might arise and receive regular updates on school issues and broader policy and practice information;
- take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO, DSL and Governors to ensure a Data Protection Act 2018 (DPA) compliant framework for storing data, but helping to ensure

that child protection is always put first and data-protection processes support careful and legal sharing of information;
- ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to child-safety first principles;
- be responsible for ensuring that all staff receive suitable training to carry out their child protection and online safety roles;
- understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident or allegation against a member of staff or other adult (see flowchart on dealing with online safety incidents – Appendix I;
- ensure suitable risk assessments are undertaken so the curriculum meets needs of pupils, including the risk of children being radicalised;
- ensure that there is a system in place to monitor and support staff (WESTCOM) who carry out internal technical online safety procedures;
- ensure Governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety;
- ensure the school website meets statutory requirements (see KAHSC guidance on statutory and desirable website requirements).

1.3 Designated Safeguarding Lead (DSL)/Online Safety Lead (OSL)

The DSL may delegate certain online safety duties e.g. to the OSL, but not the day-to-day responsibility; this assertion and all quotes below are taken from Keeping Children Safe in Education. Where the online-safety co-ordinator is not the named DSL or deputy DSL, there must be a regular review and open communication between these roles to ensure that the DSL's clear overarching responsibility for online safety is not compromised.

The Designated Safeguarding Lead/Online Safety Lead will:

- take lead responsibility for safeguarding and child protection (including online safety);
- ensure an effective approach to online safety is in place that empowers the school to protect and educate the whole school community in their use of technology and establish mechanisms to identify, intervene in and escalate any incident where appropriate;
- promote an awareness and commitment to online safety throughout the school community with strong focus on parents, who are often appreciative of school support in this area, but also including 'hard-to-reach' parents;
- liaise with other agencies in line with 'Working together to Safeguard Children' statutory guidance;
- take day-to-day responsibility for online safety issues and be aware of the potential for serious child protection concerns;
- ensure that online safety education is embedded in line with DfE guidance 'Teaching Online Safety in schools' across the curriculum (e.g. by use of the UKCIS framework 'Education for a Connected World') and beyond, in the wider school community;
- work with the Head teacher, Data Protection Officer, Governors and the school ICT technical staff to ensure a DPA compliant framework for storing data, helping to ensure that child protection is always at the fore and data protection processes support careful and legal sharing of information;
- keep up to date with the latest local and national trends in online safety;
- review and update this Policy and procedures, other online safety documents (e.g. Acceptable Use Agreements) and the strategy on which they are based (in line with Policies and procedures for behaviour and child protection) and submit for review on a regular basis to the Governors/Trustees;
- liaise with school technical, pastoral, and support staff as appropriate;
- communicate regularly with SLT and the designated online safety Governor/committee to discuss current issues (anonymised), 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 and that these are logged in the same way as any other child protection incident;
- oversee and discuss 'appropriate filtering and monitoring' with Governors (both physical and technical) and ensure staff are aware of its necessity;
- ensure the DfE guidance on sexual violence and harassment is followed throughout the school and that

staff adopt a zero-tolerance approach to this as well as to bullying generally;
- facilitate training and advice for staff and others working in the school:
  - all staff must read and understand KCSiE Part one and all those working with children, Annex A;
  - it would also be advisable for all staff to be aware of Annex C (Online safety);
  - cascade knowledge of risks and opportunities throughout the organisation;
- 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

Responsibilities of the Network Manager/ICT Technician include:

- all as listed in the 'all staff' section above;
- reporting any online safety related issues that arise, to the DSL/OSL in the first instance;
- keeping up to date with the school's Online safety Policy and technical information to effectively carryout their online safety role and to inform and update others as relevant;
- working closely with the DSL/OSL/DPO to ensure that school systems and networks reflect school Policy;
- ensuring that the above stakeholders understand the terms of existing services and how any changes to these systems (especially in terms of access to personal and sensitive records/data and to systems such as YouTube mode, web filtering settings, sharing permissions for files on cloud platforms etc.) might affect the system functions and safety online;
- supporting and providing advice on the implementation of 'appropriate filtering and monitoring' as determined by the DSL and Senior Leadership Team;
- ensuring that users may only access the school's networks through an authorised and properly enforced password protection procedures, in which passwords are regularly changed;
- ensuring 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;
- ensuring that access controls/encryption exist to protect personal and sensitive information held on school-owned devices;
- monitoring the use of the network/remote access/email and social media presence and that any misuse/attempted misuse is reported to the DSL/OSL in line with school Policy;
- ensuring that appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster and to complement the business continuity process;
- maintaining up-to-date documentation of the school's online security and technical procedures;
- working with the Head teacher to ensure the school website meets statutory DfE requirements;
- reporting online safety issues that come to their attention in line with school Policy.

1.5 Data Protection Officer (DPO)

The DPO will be familiar with references to the relationship between data protection and safeguarding in key DfE documents 'Keeping Children Safe in Education' and 'Data protection: a toolkit for schools'.

Neither the Data Protection Act 2018 nor GDPR prevent, or limit, the sharing of information for the purposes of keeping children safe. Information which is sensitive and personal will be treated as 'special category personal data' for the purposes of compliance with DPA 2018. Legal and secure information sharing between schools, Children's Social Care and other local agencies is essential for keeping children safe and ensuring they get the support they need. Information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information **must not** be allowed to stand in the

way of promoting the welfare and protecting the safety of children. As with all data sharing, appropriate organisational and technical safeguards will be in place.

Other responsibilities of the DPO include:

- working with the DSL, Head teacher and Governors to ensure frameworks are in place for the protection of data and of safeguarding information sharing as outlined above;
- ensuring that all access to safeguarding data is limited as appropriate, monitored and audited.

1.6 All Staff

It is the responsibility of all staff to:

- understand that online safety is a core part of safeguarding; as such it is part of everyone's role. Never think that 'someone else will pick it up';
- know who the Designated Safeguarding Lead and Online Safety Lead are;
- read and understand Part 1, Annex A and Annex C of 'Keeping Children Safe in Education' statutory guidance – whilst Part 1 is statutory for all staff, Annex A for SLT and whose working directly with children, it is good practice for all staff to read all three sections;
- read, understand and help promote the school's Online Safety Policy and procedures in conjunction with the Child Protection and other related school Policies and procedures;
- read, sign and follow the school Staff Acceptable Use Agreement and staff Code of Conduct;
- be aware of online safety issues related to the use of mobile technology e.g. phones, cameras and other hand-held devices and follow school procedures in relation to these devices;
- ensure the security of their username and password for the school system, not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security. Passwords will be changed on a regular basis and at least every 6 months;
- record online safety incidents in the same way as any child protection incident and report incidents to the DSL/OSL in accordance with school procedures;
- notify the DSL/OSL if policy does not reflect practice in the school and follow escalation procedures if concerns are not promptly acted upon;
- identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise;
- whenever overseeing the use of technology (devices, the Internet, new technology such as augmented reality, etc.) in school or setting as homework tasks, encourage sensible use, monitor what pupils are doing and consider potential dangers and the age appropriateness of websites (check what appropriate filtering and monitoring processes are in place);
- carefully supervise and guide pupils when engaged in learning activities involving online technology, supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law;
- prepare and check all online source and resources before using in the classroom;
- encourage pupils to follow their Acceptable Use Agreement, regularly remind them about it and enforce school sanctions where there is a breach of the Agreement;
- notify the DSL/OSL of new trends and issues before they become a problem;
- take a zero-tolerance approach to bullying and low-level sexual harassment either offline or online;
- receive and act upon regular updates from the DSL/OSL and have a healthy curiosity for online safety issues;
- model safe, responsible and professional behaviours in their own use of technology. This includes outside the school hours and site, and on social media, in all aspects upholding the reputation of the school and the professional reputation of all staff;
- 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.

1.7 PSHE/RSHE Lead(s)

Responsibilities of PSHE/RSHE Leads include:

- all as listed in the 'all staff' section above;
- ensuring that consent, mental wellbeing, healthy relationships and staying safe online is embedded into the PSHE/Relationships education, relationships and sex education (RSE) and health education curriculum. This will include being taught what positive, healthy and respectful online relationships look like, the effects of the pupils' online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers will address online safety and appropriate behaviour in an age appropriate way that is relevant to their pupils' lives (KCSiE);
- complementing the computing curriculum which covers the principles of online safety at all key stages, with progression in the content to reflect the different and escalating risks that pupils face. This includes how to use technology safely, responsibly, respectfully and securely, and where to go for help and support when the pupil has concerns about content or contact on the Internet or other online technologies;
- working closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messages within PSHE/RSHE.

1.8 Computing/Subject Lead(s)

Responsibilities of the Computing Lead include:

- all as listed in the 'all staff' section above;
- the overseeing delivery of the online safety element of the Computing curriculum in accordance with the national curriculum;
- working closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messages within Computing;
- collaboration with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with Acceptable Use Agreements.

1.9 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 age-appropriate 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. As with consent on data (privacy notices) Agreements must be written in terms the EYFS/KS1 child can understand; (NB. at EYFS and KS1 parents can sign on behalf of the pupils but pupils must understand the Agreement)
- ensure the security of their username and password for the school system, not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security;
- 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;

1.10 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, websit and information about national/local online safety campaigns/literature.*

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/Facebook 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;
- Promote positive online safety and model safe, responsible and positive behaviours in their own use of technology (including social media) by ensuring 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.

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 regular training available to staff on online safety issues and the school's online safety education programme & during E -safety Week.
- provides, as part of the induction process, all new staff (including those on university/college placements and work experience) and volunteers with information and guidance on the Online Safety Policy and procedures the school's Acceptable Use Agreements.

2.2 Parent Awareness and Training

This school operates a rolling programme of advice, guidance and training for parents, including:

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

3. Teaching and Learning

The following subjects have the clearest online safety links (see relevant role descriptors above for more information):

- Personal, Social and Health Education (PSHE)
- Relationships education, relationships and sex education (RSE) and health
- Computing
- Citizenship

It is, however, the role of all staff to identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting subject lead staff and making the most of unexpected learning opportunities as they arise.

Whenever overseeing the use of technology (devices, the Internet, new technology such as augmented reality, etc) in school or setting as homework tasks, all staff will encourage sensible use, monitor what pupils are doing and consider potential dangers and the age appropriateness of websites.

Equally, all staff should carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright, plagiarism and data law.

We recognise that online safety and broader digital resilience must be included throughout the curriculum.

Annual reviews of curriculum plans / schemes of work (including for SEND pupils) are used as an opportunity to assess the key areas of Self-image and Identity, Online relationships, Online reputation, Online bullying, Managing online information, Health, Wellbeing and lifestyle, Privacy and security, and Copyright and ownership.

3.1 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.*

3.2 How Internet Use Enhances Learning

This school:

- Has a clear, progressive 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 or the CLICK CEOP button.

- 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 network.
- 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.

3.3 Pupils with Additional Needs

- A fundamental part of teaching online safety is to check pupil's understanding and knowledge of general personal safety issues. 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.
- Rules are very helpful to all pupils and it is important to achieve consistency of how rules can be applied.
- As consistency is so important for these pupils, there is a need to establish online safety rules for school that are similar to those for home. We will work with parents to build this consistency.
- There will always be exceptions to rules and if this is the case, then these pupils will need to have additional explanations about why rules might change in different situations i.e. why it is ok to give your name and address to an adult if you are lost in town, but not when using the internet.
  Visual support is usually important to help most pupils' understanding but some areas of this topic are quite abstract in nature and difficult to represent visually i.e.
  - Uncomfortable
  - Smart
  - Stranger
  - Friend

  In these cases we will ask pupils to produce a drawing or write a mini-class dictionary that describes and defines these words in their own terms where necessary.

- This group of pupils are vulnerable to poor social understanding that may leave them open to risks when using the internet individually, but also when with peers. Adults will plan group interactions carefully when raising awareness of internet safety.

4. Handling online safety concerns and incidents

Our staff recognise that online safety is only one element of the wider safeguarding agenda as well as being a curriculum strand of Computing, PSHE/RSHE and Citizenship.

General concerns will be handled in the same way as any other child protection concern. Early reporting to the DSL/OSL is vital in order to ensure that the information contributes to the overall picture or highlights what might not yet be a problem.

Support staff will often have a unique insight and opportunity to find out about issues first in the playground, corridors, toilets and other communal areas outside the classroom (particularly relating to bullying and sexual harassment and violence).

Procedures for dealing with online safety, concerns and incidents are detailed in the following Policies:

- Child Protection Policy and procedures
- Peer on peer abuse Policy and procedures

- Whole School Behaviour Policy and procedures (includes anti-bullying procedures)
- Acceptable Use Agreements
- Prevent Risk Assessment
- Data Protection Policy, agreements and other documentation (e.g. privacy statement, consent forms for data sharing image use etc.)

We are committed to taking all reasonable precautions to ensure online safety but recognise that incidents will occur both inside and outside school. All members of the school community are encouraged to report issues swiftly to school staff so that they can be dealt with quickly and sensitively through the school's escalation processes.

Any suspected online risk or infringement should be reported to the DSL/OSL on the same day wherever possible or, if out of school, the following school day.

Any concern/allegation about misuse by staff or other adult in school will always be referred directly to the Head teacher unless the concern is about the Head teacher, in which case, the complaint will be directed to the Chair of Governors. Staff may also use the NSPCC Whistleblowing Helpline. Call 0800 028 0285 or email: help@nspcc.org.uk.

The school will actively seek support from other agencies as needed (i.e. Local Authority Safeguarding Hub, UK Safer Internet Centre's Professionals' Online Safety Helpline (03443814772), NCA CEOP, Cumbria Police Prevent Officer, Cumbria Police, Internet Watch Foundation (IWF)). We will inform parents of online safety incidents involving their child and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly disturbing or is considered illegal. See Sections below for procedures for dealing with sexting and upskirting and online bullying.

- In this school there is strict monitoring and application of the Online Safety Policy and a differentiated and appropriate range of sanctions.
- All members of the school community will be informed about the procedure for reporting online safety concerns (such as breaches of filtering, cyberbullying, illegal content etc.).
- 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 or 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.

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence, and protect those carrying out the investigation. More than one member of staff should be involved in the investigation which should be carried out on a "clean" designated computer.

Incidents will be dealt with as soon as possible in a proportionate manner through normal behaviour/disciplinary procedures. It is important that, where necessary, members of the school community are made aware that incidents have been dealt with.

4.1 Sexting

Where incidents of Sexting are discovered, we will refer to the UK Council for (UKCIS) guidance on Sexting (also referred to as 'Youth produced sexual imagery') in schools. A copy of this document is available from the school office. Where one of the parties is over the age of 18, rather than sexting, we will refer to it as child sexual abuse.

All staff and other relevant adults have been issued with a copy of the UKCIS overview document (Sexting: how to respond to an incident) in recognition of the fact that it is generally someone other than the DSL or OSL who will first become aware of an incident, Staff, other than the DSL must not attempt to view, share or delete the image or ask anyone else to do so but must report the incident to the DSL as soon as possible.

It is the responsibility of the DSL to follow the guidance issued by UKCIS, decide on the next steps and whether to involve other agencies as appropriate.

It is important to understand that whilst sexting is illegal, pupils should be encouraged to discuss with staff situations if they have made a mistake or had a problem with this issue.

4.2 Online bullying

Online bullying (also known as cyberbullying) will be treated in the same way as any other form of bullying and the Whole School Behaviour Policy and procedures will be followed in relation to sanctions taken against the bully. It is important not to treat online bullying separately to offline bullying and to recognise that some bullying will have both online and offline elements. Support will be provided to both the victim and the perpetrator. In some cases, it may be necessary to inform or involve the Police.

Many young people and adults find that using the Internet and mobile phones is a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. When children are the target of bullying via mobile phones, gaming or the Internet, they can often feel very alone, particularly if the adults around them do not understand cyberbullying and its effects. A once previously safe and enjoyable environment or activity can become threatening, harmful and a source of anxiety. It is essential that young people, school staff and parents understand how cyberbullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety.

There are several statutory obligations on schools in relation to behaviour which establish clear responsibilities to respond to bullying. In particular, section 89 of the Education and Inspections Act 2006:

- every school must have measures to encourage good behaviour and prevent all forms of bullying amongst pupils. These measures should be part of the school's Behaviour Policy which must be communicated to all pupils, school staff and parents;
- gives Head teachers the ability to ensure that pupils behave when they are not on school premises or under the lawful control of school staff.

Where bullying outside school (such as online or via text) is reported to the school, it will be investigated and acted on.

Although bullying in itself is not a specific criminal offence in the UK, it is important to bear in mind that some types of harassing or threatening behaviour or communications could be a criminal offence, for example under the Protection from Harassment Act 1997, the Malicious Communications Act 1988, the Communications Act 2003, and the Public Order Act 1986. If school staff feels that an offence may have been committed, they should seek assistance from the Police.

DfE and Childnet have produced resources and guidance that we expect staff to use to give practical advice and guidance on cyberbullying:

- Cyberbullying (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 and procedures.
- There are clear procedures in place to support anyone in the school community affected by cyberbullying.
- All incidents of cyberbullying reported to the school will be recorded.
- There will be clear procedures in place to investigate incidents or allegations of cyberbullying.
- Pupils, staff and parents will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.

- Pupils, staff and parents will be required to work with the school to support the approach to cyberbullying and the school's online safety ethos.
- Sanctions for those involved in cyberbullying may include:
  - The bully will be asked to remove any material deemed to be inappropriate or offensive.
  - A service provider may be contacted to remove content if the bully refuses or is unable to delete content.
  - Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance with the Whole School Behaviour Policy, Acceptable Use Agreement and Disciplinary Procedures.
  - Parents of pupils will be informed.
  - The Police will be contacted if a criminal offence is suspected.

4.3 Sexual violence and harassment

DfE guidance on sexual violence and harassment is referenced in 'Keeping Children Safe in Education' and separate guidance exists on this issue 'Sexual violence and sexual harassment between children in schools and colleges'. All staff are aware of this guidance.

We take all forms of sexual violence and harassment seriously and will act appropriately on information which suggests inappropriate behaviour regardless of the considered seriousness. Any incident of sexual harassment or violence (online or offline) must be reported to the DSL at the earliest opportunity. The DSL will follow the guidance as outlined in the Child Protection Policy and procedures.

4.4 Misuse of school technology (devices, systems, networks or platforms)

Clear and well communicated rules and procedures are essential to govern pupil and adult use of school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

These rules are defined in the relevant Acceptable Use Agreements as provided to pupils, staff and Governors.

Where pupils contravene these rules, the Whole School Behaviour Policy and procedures will be applied; where staff contravene these rules, action will be taken as outlined in the staff code of conduct and, where necessary, the school disciplinary procedures.

The school reserves the right to withdraw, temporarily or permanently, any or all access to such technology or the right to bring mobile technology devices onto school property.

4.5 Social media incidents

See also Section 9. below. Social media incidents are governed by Acceptable Use Agreements. Breaches will be dealt with in line with these procedures, the Whole School Behaviour Policy and procedures (for pupils) and the staff Code of Conduct/Disciplinary procedures (for staff and other adults).

Where an incident relates to an inappropriate, upsetting, violent or abusive social media post by an identifiable member of the school community, we will request that the post be deleted and will expect this to the actioned promptly.

Where an offending post has been made by a third party or is anonymous, the school may report it to the hosting platform, the Police or may contact the Professionals' Online Safety Helpline (UK Safer Internet Centre) for support or assistance in accelerating the process of removal.

5. Data protection and data security

All pupils, staff, Governors, parents and other adults working in or visiting school are bound by the school's Data Protection Policy and procedures a copy of which is available from the school office.

There are references to the relationship between data protection and safeguarding in key DfE documents i.e. 'Keeping Children Safe in Education' and 'Data protection: a toolkit for schools' which the DPO and DSL will seek to apply.

The Head teacher, DPO and Governors work together to ensure a DPA compliant framework for storing data, but which ensures that child protection is always the primary consideration and data protection processes support careful and legal sharing of information. The Data Protection Act 2018 does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Information which is sensitive and personal will be treated as 'special category personal data' for the purposes of compliance with the DPA. Legal and secure information sharing between schools, Children's Social Care and other local agencies is essential for keeping children safe and ensuring they get the support they need. Information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information **must not** be allowed to stand in the way of promoting the welfare and protecting the safety of children. As with all data sharing, appropriate organisational and technical safeguards will be in place.

All pupils, staff, Governors, volunteers, contractors and parents are bound by the school's Data Protection Policy and procedures.

5.1 Maintaining Information Systems Security

Local Area Network (LAN) security issues include:

- Users must act reasonably e.g. the downloading of large files or viewing sporting events during the working day will affect the service that others receive.
- Users must take responsibility for their network use. For staff, flouting the school Acceptable Use Agreement may be regarded as a reason for dismissal.
- Workstations should be secured against user mistakes and deliberate actions.
- Servers will be located securely and physical access restricted.
- The server operating system is secured and kept up to date.
- Virus protection for the whole network is installed and current.
- Access by wireless devices will be proactively managed and secured with a minimum of WPA2 encryption.

Wide Area Network (WAN) security issues include:

- Broadband firewalls and local CPEs (Customer Premises Equipment) are configured to prevent unauthorised access between schools.
- Decisions on WAN security are made in partnership between school and our network provider.

The following statements apply in our school:

- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Personal data sent over the Internet or taken off site will be encrypted.
- Portable media may not be used without specific permission followed by an anti-virus/malware scan.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the school's network will be regularly checked.
- The ICT coordinator/network manager will review system capacity regularly.
- Use of user logins and passwords to access the school network will be enforced

The Head teacher, Data Protection Officer and Governors work together to ensure a DPA compliant framework for storing data, but which ensures that child protection is always put first and data protection processes support careful and legal sharing of information.

5.2 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;**
- **logs are maintained of access by users and of their actions while users of the system.**

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 emails.

The management of password security will be the responsibility of Westcom

Responsibilities:

All users (adults and young people) will have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

Passwords for new users, and replacement passwords for existing users will be allocated by Westcom.

Users will change their passwords every 90 days

Training/Awareness:

It is essential that users are made aware of the need to keep passwords secure, and the risks attached to unauthorised access/data loss. This should apply to even the youngest of users, even if class log-ons are being used.

Members of staff will be made aware of the school's password security procedures:

- at induction;
- through the school's Online Safety Policy and procedures;
- through the Acceptable Use Agreement;

Pupils will be made aware of the school's password security procedures:

- in ICT and/or Online Safety lessons
- through the Acceptable Use Agreement

The following rules apply to the use of passwords

passwords must be changed every 90 days

- the last four passwords cannot be re-used;
- the password should be a minimum of 8 characters long and must include three of – uppercase character, lowercase character, number, special character;
- the account should be "locked out" following six successive incorrect log-on attempts;
- temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on;
- passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption);
- requests for password changes should be authenticated by (the responsible person) to ensure that the new password can only be passed to the genuine
- The "master/administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Head teacher or other nominated senior leader and will be kept secure.

Audit/Monitoring/Reporting/Review:

A.Mann/S.Hughes will ensure that full records are kept of:

- User Ids and requests for password changes;
- User log-ons;
- Security incidents related to this Policy and procedures.

In the event of a serious security incident, the police may request and will be allowed access to passwords used for encryption. Local Authority Auditors also have the right of access to passwords for audit investigation purposes.

User lists, IDs and other security related information must be given the highest security classification and stored in a secure manner. These records will be reviewed by (Online Safety Coordinator/Online Safety Committee/Online Safety Governor) annually.

5.3 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.
- Access in school to external personal email accounts may be blocked.
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be.
- The forwarding of chain messages is not permitted.
- 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 (email, chat,) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat/social networking programmes must not be used for these communications.
- Whole class or group email addresses will be used at KS1, while pupils at KS2 and above will be provided with individual school email addresses for educational use.
- Pupils will be taught about email safety issues, such as the risks attached to the use of personal details. They will 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 (Westcom) ensures mail is virus checked (ingoing and outgoing), includes spam filtering and backs emails up daily.

5.4 Emailing Personal, Sensitive, Confidential or Classified Information

Staff or pupil personal data should never be sent/shared/stored in emails and any data must be encrypted prior to being sent.

- 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;
- The use of Hotmail, BTInternet, G-mail or any other Internet based webmail service for sending email containing sensitive information is not permitted;
- Where your conclusion is that email must be used to transmit such data:
  - Obtain express consent from your manager to provide the information by email;
  - Exercise caution when sending the email and always follow these checks before releasing the email:
    - Verify the details, including accurate email address, of any intended recipient of the information;
    - Verify (by phoning) the details of a requestor before responding to email requests for information;
    - Do not copy or forward the email to any more recipients than is necessary.
  - Do not send the information to any person whose details you have been unable to separately verify (usually by phone);
  - 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) e.g. by telephone or in writing;
  - Do not identify such information in the subject line of any email;
  - Request confirmation of safe receipt.

5.5 Zombie Accounts

- We ensure that all user accounts are disabled once the member of the school has left;
- Prompt action on disabling accounts will prevent unauthorised access;
- Regularly change generic passwords to avoid unauthorised access (Microsoft© advise every 42 days).

6. School Website

The school website is a key public-facing information portal for the school community (both existing and prospective stakeholders) with a key reputational value. Shelagh Hughes has day to day editorial responsibility for online content published by the school on the school website and will ensure that content published is accurate and appropriate.

The DfE has determined information which must be available on a school website. 'What schools must publish online'.
Where other staff submit information for the website, they are asked to consider the following principles:

- The contact details on the website are the school address, email and telephone number. Staff, Governors or pupils' personal information are not published.
- Email addresses will be published carefully online, to avoid being harvested for spam (e.g. by replacing '@' with 'AT').
- The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy procedures and copyright.
- Where pupil work, images or videos are published on the website, their identities are protected and full names are not published (remember also not to save images with a filename that includes a pupil's full name).
-

6.1 Use of Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, pupils and parents need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement procedures to reduce the likelihood of the potential for harm:

- We gain parental permission for the use of digital photographs or video involving their child as part of the school agreement form when their child joins the school. This is a once in a school lifetime consent. Parents are required to inform the school if their consent changes.
- 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;
- The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose;
- 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.
- If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long term use.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Pupil's work, where named, can only be published with the permission of the pupil and parents.

7. Cloud Platforms

Many schools are recognising the benefits of cloud computing platforms, not just for cost savings, but to enhance teaching and learning. This school adheres to the principles of the Department for Education document 'Cloud computing services: guidance for school leaders, school staff and governing bodies'. As more and more systems move to the cloud, it becomes easier to share and access data. Our Data Protection Policy and procedures includes the use of Cloud services.

For online safety, basic rules of good password management, expert administration and training is used to keep staff and pupils safe and to avoid incidents. The DPO and network manager will analyse and document systems and procedures before they are implemented and regularly review them.

The following principles apply:

- Privacy statements inform parents and children when and what type of data is stored in the cloud.
- The DPO approves new cloud systems, what may or may not be stored in them and by whom. This information is included in a DPIS (data protection impact statement).
- Regular training ensures all staff understand sharing functionality and this is audited to ensure that pupil data is not shared by mistake. Open access or widely shared folders are clearly marked as such.
- Pupils and staff are only given access and/or sharing rights when they can demonstrate an understanding of what data may be stored and how it can be seen.
- Two-factor authentication is used for access to staff or pupil data.
- Pupil images/videos are only made public with parental consent.
- Only school-approved platforms are used by students or staff to store pupil work.
- All stakeholders understand the difference between consumer and education products (e.g. a private Gmail account or Google Drive and those belonging to a managed educational domain).

7.1 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. Staff will obtain documented consent from the Senior Leadership Team before using Social Media tools in the classroom.
- Staff official blogs or wikis should be password protected and run from the school website with approval from the Senior Leadership Team. Members of staff are advised not to run social network spaces for pupil use on a personal basis.
- 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.

- Pupil will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.
- 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

7.2 Managing Filtering

- The school's broadband access will include filtering appropriate to the age and maturity of pupils.
- The school will work with the Westcom to ensure that filtering procedures are continually reviewed.
- The school will have a clear procedure for reporting breaches of filtering. All members of the school community (all staff and all pupils) will be aware of this procedure.
- 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 filtering system will block all sites on the Internet Watch Foundation (IWF) list
- Changes to the school filtering procedures will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Senior Leadership Team.
- The School Senior Leadership Team will ensure that regular 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 IWF Cumbria Police or CEOP.
- The school's access strategy will be designed by educators to suit the age and curriculum requirements of the pupils, with advice from network managers.

7.3 Managing Video conferencing

- External IP addresses will not be made available to other sites.
- Video conferencing contact information (e.g zoom details) will not be put on the school Website..
- Conference supervisors need to be familiar with how to use the video conferencing software and apps, particularly how to end a call if at any point any person taking part becomes unhappy with the content of the conference

Users:

- Pupils will ask permission from a teacher before making or answering a videoconference call.
- Videoconferencing will be supervised appropriately for the pupils' age and ability.
- Parent's consent should be obtained prior to children taking part in videoconferences, especially those with end-points outside of the school.
- Unique log on and password details for the educational videoconferencing services should only be issued to members of staff and kept secure.

Content:

- When recording a videoconference session, permission should be given by participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference. Recorded material shall be stored securely.
- Videoconferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity.
- If third party materials are to be included, check that recording is acceptable to avoid infringing the third party intellectual property rights.
- Establish dialogue with other conference participants before taking part in a videoconference. If it is a non-school site it is important to check that they are delivering material that is appropriate for your class.

7.4 Webcams and CCTV

- We do not use publicly accessible webcams in school.
- Webcams in school are only ever used for specific learning purposes, i.e. monitoring hens' eggs and never using images of children unless we have consent from parents.
- Misuse of the webcam by any member of the school community will result in sanctions.
- Consent is sought from parents and staff on joining the school, in the same way as for all images.

7.5 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.

7.6 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.**

When personal data is stored on any portable computer system, USB stick or any other removable media:

- the data must be encrypted and password protected;
- the device must be password protected (many memory sticks/cards and other mobile devices cannot be password protected);
- the device must offer approved virus and malware checking software;
- the data must be securely deleted from the device, in line with school procedures (below) once it has been transferred or its use is complete.

7.7 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) ICO Guidance - Data Protection Act 1998
- 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.**

- Any redundant ICT equipment being considered for sale/gift will have been subject to a recent electrical safety check and hold a valid PAT certificate.

8. Policy Decisions

8.1 Authorising Internet Access

- The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.
- 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.
- Parents will be informed that pupils will be provided with supervised Internet access appropriate to their age and ability.
- When considering access for vulnerable members of the school community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the pupil(s).

According to Setting Type:

- 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 allowed to use the internet unsupervised where appropriate(as the system is filtered), however they will report any issues in accordance with the *Think then Click rules* . Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary.

8.2 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.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Cumbria Police.
- Methods to identify, assess and minimise risks will be reviewed regularly.

8.3 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:

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					✓	
Online gaming (educational)			✓			
Online gaming (non-educational)			✓			
Online gambling					✓	
Online shopping/commerce			✓			
File sharing			✓			

User Actions	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Use of social networking sites		✓			
Use of video broadcasting e.g. Youtube		✓			

8.4 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)	Adverts Spam Sponsorship Personal Info	Violent/hateful content	Pornographic or unwelcome sexual content	Bias, Racist or Misleading info or advice
Contact (Child as participant)	Tracking Harvesting personal info	Being bullied, harassed or stalked	Meeting strangers, Being groomed	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

Byron Review (2008):

8.5 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.
- In this school there is strict monitoring and application of the Online Safety Policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions
- All members of the school community will be informed about the procedure for reporting online safety concerns (such as breaches of filtering, cyber-bullying, illegal content etc.).
- 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.

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. More than one member of staff should be involved in the investigation which should be carried out on a "clean" designated computer.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows

Pupils **Actions / Sanctions**

Incidents:	Refer to class teacher/tutor	Refer to Head of Department/Head of Year/other	Refer to Head teacher	Refer to Police	Refer to technical support staff for action re filtering/security etc.	Inform parents	Removal of network / internet access rights	Warning	Further sanction e.g. detention/exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).		✓	✓	✓					
Unauthorised use of non-educational sites during lessons	✓	✓	✓		✓	✓		✓	✓
Unauthorised use of mobile phone / digital camera / other handheld device	✓					✓		✓	
Unauthorised use of social networking / instant messaging / personal email	✓	✓	✓		✓	✓		✓	✓
Unauthorised downloading or uploading of files	✓					✓		✓	
Allowing others to access school network by sharing username and passwords	✓	✓			✓	✓		✓	
Attempting to access or accessing the school network, using another pupil's account	✓	✓			✓	✓		✓	
Attempting to access or accessing the school network, using the account of a member of staff	✓	✓			✓	✓		✓	✓
Corrupting or destroying the data of other users	✓					✓		✓	
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✓	✓			✓	✓		✓	✓
Continued infringements of the above, following previous warnings or sanctions	✓	✓		✓	✓	✓		✓	✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✓	✓			✓	✓		✓	✓
Using proxy sites or other means to subvert the school's filtering system	✓	✓	✓	✓	✓	✓		✓	✓

Accidentally accessing offensive or pornographic material and failing to report the incident	✓	✓	✓		✓	✓		✓	
Deliberately accessing or trying to access offensive or pornographic material	✓	✓	✓		✓	✓		✓	✓
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	✓	✓	✓			✓			

Staff **Actions / Sanctions**

Incidents:	Refer to line manager	Refer to Head teacher	Refer to LA/HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		✓	✓	✓	✓	✓	✓	✓
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	✓	✓				✓		
Unauthorised downloading or uploading of files	✓	✓			✓	✓		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	✓	✓				✓		
Careless use of personal data e.g. holding or transferring data in an insecure manner	✓	✓				✓		
Deliberate actions to breach data protection or network security rules	✓	✓				✓	✓	✓
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	✓	✓		✓	✓	✓	✓	✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✓	✓	✓	✓	✓	✓	✓	✓
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils	✓	✓	✓	✓	✓	✓	✓	✓
Actions which could compromise the staff member's professional standing	✓	✓				✓		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✓	✓				✓		
Using proxy sites or other means to subvert the school's filtering system	✓	✓			✓	✓	✓	✓
Accidentally accessing offensive or pornographic material and failing to report the incident	✓	✓				✓		
Deliberately accessing or trying to access offensive or pornographic material	✓	✓	✓	✓	✓	✓	✓	✓
Breaching copyright or licensing regulations	✓	✓			✓	✓		
Continued infringements of the above, following previous warnings or sanctions	✓	✓				✓	✓	✓

8.6 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.
- Pupils, staff and parents will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Pupils, staff and parents will be required to work with the school to support the approach to cyber-bullying and the school's online safety ethos.
- Sanctions for those involved in cyber-bullying may include:
  - The bully will be asked to remove any material deemed to be inappropriate or offensive.
  - A service provider may be contacted to remove content if the bully refuses or is unable to delete content.
  - Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance with the Whole School Behaviour Policy, Acceptable Use Agreement and Disciplinary Procedures.
  - Parents of pupils will be informed.
  - The Police will be contacted if a criminal offence is suspected.

8.7 Managing Mobile Phones and Personal Devices

- We do not permit the use of mobile phones by children in school unless for very special circumstances agreed by the head teacher.
- Children who bring a mobile to school must leave it in the office and collect at the end of the day- this will be arranged with parents.
- The use of mobile phones and other personal devices by pupils and staff in school will be decided by the school and covered in the school Acceptable Use Agreement.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school discipline/Behaviour Policy.
- The school reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable materials, including those which promote pornography, violence or bullying. Staff mobiles or hand-held devices may be searched at any time as part of routine monitoring.
- School staff may confiscate a phone or device if they believe it is being used to contravene the school's behaviour Policy or bullying procedures.
- If there is suspicion that the material on the mobile may provide evidence relating to a criminal offence the phone will be handed over to the police for further investigation.
- The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided, except where it has been explicitly agreed otherwise by the Head teacher. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Head teacher is authorised to withdraw or restrict authorisation for use at any time if it is deemed necessary. Where permission is given by the Head teacher, images or videos taken on mobile phones or personally-owned mobile devices must be uploaded to the network and then removed from the device as soon as practically possible.
- Electronic devices of all kinds that are brought in to school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.
- Where parents or pupils need to contact each other during the school day, they should do so only through the School's telephone. Staff may use their phones during break times if not on duty and at other times with permission from the head teacher.

- Mobile phones and personal devices are not permitted to be used in certain areas within the school site such as changing rooms, toilets and swimming pools.

Pupils use of personal devices:

- The school strongly advises that pupil mobile phones should not be brought into school. However, the school accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety. If this is the case, the circumstances should be discussed with the class teacher and the normal rules regarding use during the school day will apply.
- If a pupil breaches the school procedures 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 in accordance with the school procedures.
- If a pupil needs to contact his/her parents they will be allowed to use a school phone. Parents are advised to contact their child via the school office.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.
- Pupils will be provided with school hand-held personal devices to use in specific learning activities under the supervision of a member of staff. Such devices will be set up so that only those features required for the activity will be enabled.

Staff use of personal devices:

- Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity unless permitted by the headteacher under exceptional circumstances (e.g whilst on a residential)
- Mobile phones and personally owned devices will be switched off or switched to 'silent' mode; Bluetooth communication should be "hidden" or switched off and mobile phones or personally owned devices will not be used during teaching periods unless permission has been given by a member of Senior Leadership Team in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or personal devices as part of an educational activity then it will only take place when approved by the Senior Leadership Team.
- 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 they should hide (by inputting 141) their own mobile number for confidentiality purposes.
- If a member of staff breaches the school Policy and procedures then disciplinary action may be taken.

	Staff & other adults				Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	✓							✓
Use of mobile phones in lessons		✓					✓	
Use of mobile phones in social time	✓						✓	
Taking photos on mobile phones or other camera devices	✓							✓
Use of hand held devices e.g. PDAs, PSPs		✓				✓		
Use of personal email addresses in school, or on school network		✓					✓	
Use of school email for personal emails		✓						✓
Use of chat rooms/facilities	✓							✓
Use of instant messaging		✓						✓
Use of social networking sites		✓						✓
Use of blogs		✓						✓

9. Communicating Policy and procedures

9.1 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.
- Pupil instruction regarding responsible and safe use will precede Internet access.
- An online safety module will be included in the PSHE, Citizenship and/or ICT programmes covering both safe school and home use.
- Online safety training will be part of the transition programme across the Key Stages and when moving between establishments.
- Online Safety rules or copies of the pupil Acceptable Use Agreement will be posted in all rooms with Internet access.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.
- Particular attention to Online Safety education will be given where pupils are considered to be vulnerable.

9.2 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.
- Staff who manage filtering systems or monitor ICT use will be supervised by the Senior Leadership Team and have clear procedures for reporting issues.
- The School will highlight useful online tools which staff should use with children in the classroom. These tools will vary according to the age and ability of the pupils.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

9.3 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 e.g. parent evenings and sports days.
- Parents will be requested to sign an Online Safety/Internet agreement.
- 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.
- Advice on useful resources and websites, filtering systems and educational and leisure activities which include responsible use of the Internet will be made available to parents.
- Interested parents will be referred to organisations listed in the "online safety Links" at Appendix K.

10. 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/Board of Directors 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.

- Parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with the school to resolve issues.
- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
- Discussions will be held with the local Police and/or the Safeguarding Hub to establish procedures for handling potentially illegal issues.
- Any issues (including sanctions) will be dealt with according to the school's disciplinary, behaviour and child protection procedures.
  All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community or which may bring the school into disrepute.

THIS PAGE IS INTENTIONALLY BLANK FOR PRINTING PURPOSES

Appendix A

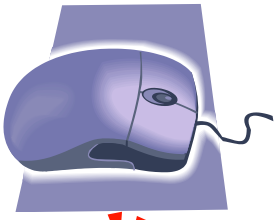
St Herbert's CE (VA)Primary & Nursey School SCHOOL ONLINE SAFETY AUDIT

This self-audit should be completed by the member of the Senior Leadership Team (SLT) responsible for Online Safety. Staff that could contribute to the audit include: Designated Safeguarding Lead, SENCO, Online Safety Coordinator, Network Manager and Head teacher.

Does the school have an Online Safety Policy and procedures	**YES / NO**
Date of latest update:	Spring 2021
Date of future review:	Spring 2022
The school Online Safety Policy and procedures was agreed by governors on:	Spring
The Policy and procedures is available for staff to access at:	Staffroom board/School Website
The Policy and procedures is available for parents to access at:	School Website/School Office
The responsible member of the Senior Leadership Team is:	A.Mann
The Governor responsible for Online Safety is:	A.Weightman
The Designated Safeguarding Lead is:	S.Hughes
The Online Safety Coordinator is:	A.Mann
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

THIS PAGE IS INTENTIONALLY BLANK FOR PRINTING PURPOSES

We only use the Internet when an adult is with



We can click on the buttons or links when we kn

We can search the internet with an

We always ask if we get lost on the I

We can send and open emails toge

We can write polite and friendly emails to peop

Think before

We ask permission before using the Internet.

We only use websites that our teacher has chose

We immediately close any webpage we don't lik

We only email people our teacher has approved

We send emails that are polite and friendly.

We never give out a home address or phone numb

We never arrange to meet anyone we don't kno

We never open emails sent by anyone we don't kn

We never use Internet chat rooms.

We tell the teacher if we see anything we are unha
with.

These rules help us to stay safe on the Internet.

Think then Click

THIS PAGE IS INTENTIONALLY BLANK FOR PRINTING PURPOSES

PUPIL ACCEPTABLE USE AGREEMENT

(St Herbert's CE(VA) Primary & Nursery & Primary Schools)

These rules will help us to be fair to others and keep everyone safe.

- 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 give my username and passwords to anyone else but my parents.
- If I think someone has learned my password then I will tell my teacher.
- I will only open/delete my own files.
- I will 'log-off' when I leave a computer.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not deliberately 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 or share my own/or others details such as name, phone number or home address.
- I will be aware of 'stranger danger' when I am communicating online and will not arrange to meet someone 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 immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online and will not show it to other pupils.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community.
- I know that my use of the school ICT systems and email can be checked and my parent 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.

✂----------

[School logo and details]

Pupil Acceptable Use – Pupil <u>and</u> Parent Agreement

Dear Parent,

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 online 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 Mrs Hughes

We have discussed this document with ……. (child name) and we agree to follow the online safety rules and to support the safe use of ICT at St Herbert's Primary & Nursery School.

Parent Name		**Pupil Class**	
Signed *(Parent)*		**Date**	
Signed *(Pupil)*		**Date**	

THIS PAGE IS INTENTIONALLY BLANK FOR PRINTING PURPOSES

Appendix F

STAFF / VOLUNTEER
ACCEPTABLE USE POLICY AGREEMENT

ICT (including data) and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This Agreement is designed to ensure that all staff and volunteers are aware of their responsibilities when using any form of ICT. This applies to ICT used in school and also applies to use of school ICT systems and equipment out of school and use of personal equipment in school or in situations related to their employment by the school. All staff and volunteers (where they are using technology in school) are expected to sign this Agreement and adhere at all times to its contents. Any concerns or clarification should be discussed with Miss Mann (Online Safety Coordinator) or Mrs Hughes (Head teacher).

This Acceptable Use Agreement is intended to ensure that:

- staff and volunteers are responsible users and stay safe while using technologies for educational, personal and recreational use;
- school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk;
- staff are protected from potential risk from the use of ICT in their everyday work and work to ensure that young people in their care are safe users.

Acceptable Use Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

Keeping Safe

- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Head teacher.
- I will only use my own user names and passwords which I will choose carefully so they cannot be guessed easily. I will also change the passwords on a regular basis.
- I will not use any other person's user name and password.
- I will not give out my own personal details, such as mobile phone number, personal email address, personal Twitter account, or any other social media link, to pupils.
- I will ensure that my data is regularly backed up.
- I will ensure that I 'log off' after my network session has finished.
- If I find an unattended machine logged on under another user's username, I will **not** continue using the machine – I will 'log off' immediately.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role or the school into disrepute.
- I will not accept invitations from school pupils to add me as a friend to their social networking sites, nor will I invite them to be friends on mine.

  As damage to professional reputations can inadvertently be caused by quite innocent postings or images, I will also be careful with who has access to my pages through friends and friends of friends, especially with those connected with my responsibilities as a Governor at the school, such as parents and their children.
- I understand that data protection requires that any personal data that I have access to must be kept private and confidential, except when it is deemed necessary that I am required by law or by school procedures to disclose it an appropriate authority.
- I will only transport, hold, disclose or share personal information about myself or others as outlined in the school personal data guidelines. I will not send personal information by email as it is not secure.
- Where personal data is transferred outside the secure school network, it must be encrypted. Personal data can only be taken out of school or accessed remotely when authorised, in advance, by the Head teacher or Governing Body. Personal or sensitive data taken off site in an electronic format must be encrypted, e.g. on a password secured laptop or memory stick. Staff leading a trip are expected to take relevant pupil information with them but this must be held securely at all times.
- I will ensure that any private social networking sites/blogs etc. that I create, or actively contribute to:
  - do not reveal confidential information about the way the school operates;
  - are not confused with my school responsibilities in any way;
  - do not include inappropriate or defamatory comments about individuals connected with the school community;
  - support the school's approach to online safety which includes 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;
- I will not try to bypass the filtering and security systems in place.

- I will only use my personal ICT in school for permissible activities and I will follow the rules set out in this agreement. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.

Promoting Safe Use by Learners

- I will support and promote the school's Online Safety, Data Protection and Behaviour Policies and help pupils to be safe and responsible in their use of ICT and related technologies.
- I will model safe use of the internet in school.
- I will educate young people on how to use technologies safely according to the school teaching programme.
- I will take immediate action in line with school procedures if an issue arises in school that might compromise a learner, user or school safety or if a pupil reports any concerns.

Communication

- I will only use the school's email/Internet/Intranet/Learning Platform and any related technologies for professional purposes or for uses deemed 'acceptable' by the Head teacher or Governing Body.
- I will communicate on-line in a professional manner and tone, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions. Anonymous messages are not permitted.
- I will not engage in any on-line activity that may compromise my professional responsibilities.
- I will not use language that could be calculated to incite hatred against any ethnic, religious or other minority group.
- I will only communicate with pupils and parents using the school's approved, secure email system(s). Any such communication will be professional in tone and manner.
- I am aware that any communication could be forwarded to an employer or governors.
- I will only use chat and social networking sites that are approved by the school.
- I will not use personal email addresses on the school ICT systems unless I have permission to do so.

Research and Recreation

- I will not browse, upload, download, distribute or otherwise access any materials which are illegal, discriminatory or inappropriate or may cause harm or distress to others.
- I will not (unless I have permission) make large downloads or uploads that might take up internet capacity.
- I know that all school ICT is primarily intended for educational use and I will only use the systems for personal or recreational use if this is allowed by the school.

Sharing

- I will not access, copy, remove or otherwise alter any other user's file, without their permission.
- I will respect the privacy and ownership of others' work online at all times and will not access, copy, remove or otherwise alter any other user's files without the owner's knowledge and permission, and will credit them if I use it.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos). If I am unsure about this, I will seek advice.
- Images of pupils and/or staff will only be taken, stored and used for professional purposes using school equipment in line with school procedures.
- I will only take images/video of pupils and staff where it relates to agreed learning and teaching activities and will ensure I have parent/staff permission before I take them.
- If images are to be published on-line or in the media I will ensure that parental/staff permission allows this.
- I will not use my personal equipment to record images/video unless I have permission to do so from the Head teacher or other Senior Manager.
- I will not keep images and/or videos of pupils stored on my personal equipment unless I have permission to do so. If this is the case, I will ensure that these images cannot be accessed or copied by anyone else or used for any purpose other than that for which I have permission.
- Where these images are published (e.g. on the school website/prospectus), I will ensure that it is not possible to idenfity the people who are featured by name or other personal information.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community.

Buying/Selling/Gaming

- I will not use school equipment for on-line purchasing, selling or gaming unless I have permission to do so.

Problems

- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the Online Safety Coordinator or Head teacher.
- I will not install any hardware of software on a computer or other device without permission of the Systems Manager.
- I will not try to alter computer settings without the permission of the Systems Manager.
- I will not cause damage to ICT equipment in school.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I understand this forms part of the terms and conditions set out in my contract of employment.
- I understand that if I fail to comply with this Acceptable Use Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors / Directors and / or the Local Authority and in the event of illegal activities the involvement of the police.

✂ ----------

Staff/Volunteer Acceptable Use Agreement

I will use the school network in a responsible way and observe all the restrictions as explained in the staff ICT Acceptable Use Agreement. I agree to use ICT by these rules when:

- ✓ I use school ICT systems at school or at home when I have permission to do so
- ✓ I use my own ICT (where permitted) in school
- ✓ I use my own ICT out of school to access school sites or for activities relating to my employment by the school

Staff/Volunteer Name			
Job Title (where applicable)			
Signed		**Date:**	

THIS PAGE IS INTENTIONALLY BLANK FOR PRINTING PURPOSES

Appendix G

GOVERNOR
ACCEPTABLE USE AGREEMENT

This Agreement is designed to ensure that all Governors are aware of their responsibilities when using any form of ICT as it relates to their role in this school. This applies to ICT used in school and also applies to use of school ICT systems and equipment out of school and use of personal equipment in school or in situations related to a Governors role in the school. All Governors (where they are using technology in relation to their role) are expected to sign this Agreement and adhere at all times to its contents. Any concerns or clarification should be discussed with Miss Mann (Online Safety Coordinator) or Mrs Hughes (Head teacher).

This Acceptable Use Agreement is intended to ensure that:

- Governors are responsible users and stay safe while using technologies for educational, personal and recreational use;
- school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk;
- Governors are protected from potential risk from the use of ICT.

School networked resources, including are intended for educational purposes and may only be used for legal activities consistent with the rules of the school. If you make a comment about the school/Trust/Local Authority you must state that it is an expression of your own personal view. Any use of the network that would bring the name of the school/Trust/Local Authority into disrepute is not permitted.

All users are required to follow the conditions laid down in the Agreement. Any breach of these conditions may lead to withdrawal of the user's access, monitoring and/or retrospective investigation of the user's use of the services, and in some instances could lead to criminal prosecution.

Personal Responsibility

- Users are responsible for their behaviour and communications.
- Governors are expected to use the resources for the purposes for which they are made available.
- It is the responsibility of the User to take all reasonable steps to ensure compliance with the conditions set out in this Agreement, and to ensure that unacceptable use does not occur.
- Users will accept personal responsibility for reporting any misuse of the network to the Head teacher/Chair of Governors

Keeping Safe

- I will not reveal any personal information (e.g. home address, telephone number, social networking details) of other users to any unauthorised person.
- I will not give out my own personal details, such as mobile phone number, personal email address, personal Twitter account, or any other social media link, to pupils.
- I will only use my own user names and passwords which I will choose carefully so they cannot be guessed easily. I will also change the passwords on a regular basis and always where I think someone may have learned my password.
- I will not use any other person's user name and password or, where they are known, pass the details to any other individual.
- I will not attempt to access other users' files or folders.
- I will ensure that I 'log off' after my network session has finished.
- If I find an unattended machine logged on under another user's username, I will **not** continue using the machine – I will 'log off' immediately.
- I will not attempt to visit websites that might be considered inappropriate or illegal. I am aware that downloading some material is illegal and the police or other authorities may be called to investigate such use.
- I will report any accidental access, receipt of inappropriate materials or filtering breaches/unsuitable websites to the Head teacher as soon as I become aware of the access/receipt.
- I will not accept invitations from pupils to add me as a friend to their social networking sites, nor will I invite them to be friends on mine.

  As damage to professional reputations can inadvertently be caused by quite innocent postings or images, I will also be careful with who has access to my pages through friends and friends of friends, especially with those connected with my responsibilities as a Governor at the school, such as parents and their children.
- I will ensure that any private social networking sites/blogs etc. that I create, or actively contribute to:
  - Do not reveal confidential information about the way the school operates
  - Are not confused with my school responsibilities in any way.

Promoting Safe Use by Learners

- I will support and promote the school's Online Safety and Data Security Policies and procedures and help pupils be safe and responsible in their use of the Internet and related technologies.

Communication

- I will not create, transmit, display or publish any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person or bring the school/Trust/Local Authority into disrepute.
- I will use appropriate language – I will remember that I am a representative of the school on a global public system. Illegal activities of any kind are strictly forbidden.
- I will not use language that could be calculated to incite hatred against any ethnic, religious or minority group.
- I am aware that email is not guaranteed to be private. Messages relating to or in support of illegal activities will be reported to the Head teacher. Anonymous messages are not permitted.
- I will not send or publish material that violates the Data Protection Act or breaches the security this Act requires for personal data, including date held in SIMS.
- I will not receive, send or publish material that violates copyright law. This includes materials sent/received using Video Conferencing or Web Broadcasting.
- I will ensure that any personal data (where the Data Protection Act applies) that is sent over the Internet (or taken off-site in any other way) will be encrypted.

Sharing

- I will not use personal digital cameras or camera phones for creating or transferring images of children or young people without the express permission of the school leadership team.

General Equipment Use

- I will not use the network in any way that would disrupt the use of the network by others.
- I will not use 'USB drives', portable hard-drives, tablets or personal laptops on the network without having them 'approved' by the school and checked for viruses.
- I will not download any unapproved software, system utilities or resources from the Internet that might compromise the network or are not adequately licensed.
- I will not attempt to harm or destroy any equipment or data of another user or network connected to the school system.
- I understand that I must comply with the Acceptable Use Agreement of any other network which is accessed via the school network.

Users of the school network are expected to inform the Head teacher/System Administrator immediately if a security problem is identified and should not demonstrate this problem to other users. Files held on the school's network will be regularly checked and monitored. Users identified as a security risk will be denied access to the network.

✂ ----------

Governor User Acceptable Use Agreement

As a school user of the network resources, I agree to follow the school rules (set out above) on its use. I will use the network in a responsible way and observe all the restrictions explained in the school Online Safety Policy and Acceptable Use Agreement. If I am in any doubt, I will consult the Head teacher.

If I do not follow the rules, I understand that this may result in loss of access to these resources as well as other disciplinary action. I realise that Governors under reasonable suspicion of misuse in terms of access or content may be placed under retrospective investigation or have their usage monitored.

Governor Name			
Signed		**Date:**	

Appendix H

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:

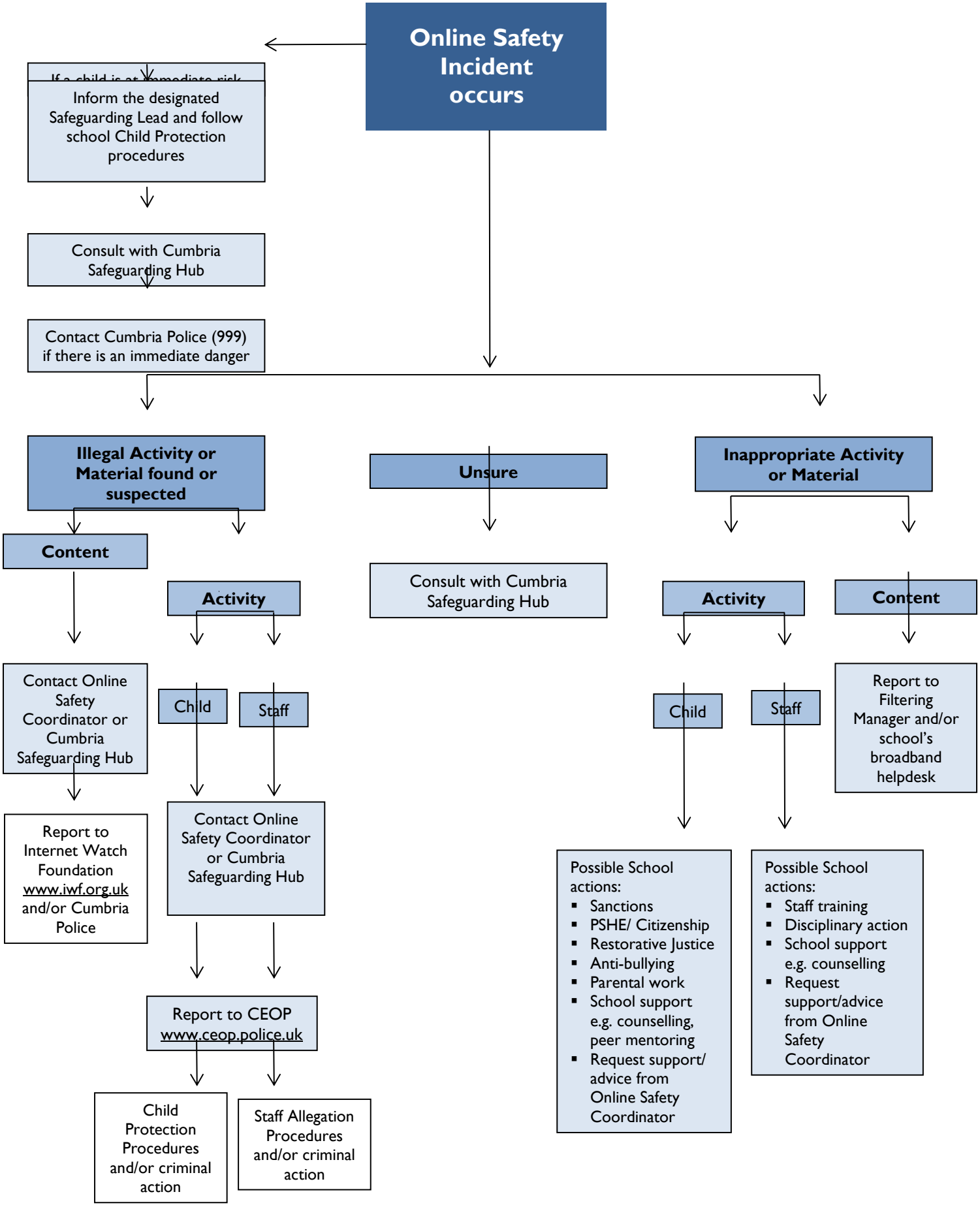
  - Always keep your profile private;
  - Never accept friends you don't know in real life;
  - Never post anything which could reveal your identity;
  - Never post anything you wouldn't want your parents to see;
  - Never agree to meet someone you only know online without telling a trusted adult;
  - 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 Click here to access.

THIS PAGE IS INTENTIONALLY BLANK FOR PRINTING PURPOSES

Appendix I

RESPONSE TO AN INCIDENT OF CONCERN



THIS PAGE IS INTENTIONALLY BLANK FOR PRINTING PURPOSES

Appendix J

ST HERBERT'S PRIMARY & NURSERY SCHOOL - ONLINE SAFETY INCIDENT LOG

Details of Online Safety incidents to be recorded by the Online Safety Coordinator. This incident log will be monitored termly by the Head teacher, member of SLT or Chair of Governors.

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

THIS PAGE IS INTENTIONALLY BLANK FOR PRINTING PURPOSES

Appendix K

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)**: Click here to access
- **Childline**: Click here to access
- **Childnet**: Click here to access
- **Internet Watch Foundation (IWF)**: Click here to access
- **Cumbria Local Safeguarding Children Board (Cumbria LSCB)**: Click here to access
- **Kidsmart**: Click here to access
- **Think U Know website**: Click here to access
- **Virtual Global Taskforce — Report Abuse**: Click here to access
- **EE Safety Education**: Click here to access
- **O2 Safety Education**: Click here to access
- **Information Commissioner's Office (ICO)** Click here to access
- **INSAFE** Click here to access
- **Anti-Bullying Network** - Click here to access
- **Cyberbullying.org** - Click here to access
- **Learning Curve Education:** Click here to access
- **UK Safer Internet Centre:** Click here to access
- **UK Council for Child Internet Safety (UKCCIS):** Click here to access
- **Wise Kids:** Click here to access
- **Teem:** Click here to access
- **Know the Net:** Click here to access
- **Family Online Safety Institute:** Click here to access
- **e-safe Education**: Click here to access
- **Facebook Advice to Parents:** Click here to access
- **Test your online safety skills:** Click here to access

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

THIS PAGE IS INTENTIONALLY BLANK FOR PRINTING PURPOSES

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.

THIS PAGE IS INTENTIONALLY BLANK FOR PRINTING PURPOSES

Appendix M

GLOSSARY OF TERMS

Becta	British Educational Communications and Technology Agency (Government agency promoting the use of information and communications technology) – *NOTE: Becta Closed in -*
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 Platform	A learning platform brings together hardware, software and supporting services to support 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