Good Shepherd Trust

life in all its fullness

Online Safety Policy and Procedures

Date of Adoption	**December 2018**
Date of Next Review	**December 2020**

POLICY

1. Definitions

This is a Trust wide policy designed to cover all of our operations. Since our area of operation covers more than one county when the document refers to Local Safeguarding Organisations it means the county in which the individual schools operate.

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 'headteacher' is used this also refers to any manager with the equivalent responsibility for children.

Wherever the term 'school' is used this refers to the Trust academies and includes any wrap around care provided and delivered by that setting such as After School Clubs and Breakfast Clubs. The proprietor is The Good Shepherd Multi Academy Trust.

This policy refers to online safety which covers all elements of working on the internet and using technology. Some existing policies refer to the e-safety policy, which is the same as this policy, these policies will be updated with the new terminology as and when they are reviewed.

2. Values

Every member of the Trust family of schools will be valued and encouraged to fulfil their potential. In our Trust we believe:

- Everyone has something to offer
- Trust, honesty, empathy and social responsibility are the Christian values that frame our work
- We are here for the whole person, spiritually, morally, educationally and socially
- In working with transparency and openness

3. Background

This policy and procedures applies to all members of the Trust 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/ work.

New technologies have become integral to the lives of children and young people in today's society, both within schools and educational settings and in their lives beyond. These technologies are powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. The Trust believes that children and young people have an entitlement to safe access to these technologies.

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 the Trust are bound. The Trust's 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 headteacher and Local Governing Body members to the senior leaders and classroom teachers, support staff, parents, members of the community and the pupils themselves.

4. What are the Risks?

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 or 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.

As well as Child Protection, Online Safety is also about Data Protection. Inappropriate use of the technology, not using passwords etc all make the personal data that the Trust holds and uses vulnerable.

It is essential that this policy is used in conjunction with other Trust policies listed below:

- Overarching Safeguarding Statement
- Child Protection Policy and Procedures
- Data Protection Policy
- Health and Safety Policy and Procedures
- Whole School Behaviour Policy
- Code of Conduct (for staff and other adults)
- Attendance Policy (including Home School Agreement)
- Website compliance document

4. Contacts

Should serious online safety incidents take place, the following external persons/agencies will be informed:

- Network Manager (Westcom) – Tel: 01900 870455 - support@west-com.co.uk
- Data Protection Officer – dataprotectionofficer@thegoodshepherdmat.co.uk
- Police
- DO (formerly (LADO):

Cumbria	Northumberland
Tel: 01768 812267 **Email:** lado@cumbria.gov.uk	**Tel:** 01670 623979 or 01670 8220386 out of hours **Email:** lado@northumberland.gov.uk

PROCEDURES

The procedures are split into three sections as follows:

The first section is the **Overarching Online Safety Principles and Practise.** It is expected that **all** staff, directors & LGB members and volunteers in the Trust and the IT Network Manager for the Trust **read, understand and abide** by these procedures.

The second section then builds on the first detailing **Specific Roles & Responsibilities** delegated to, or required by directors, staff, teaching staff, headteachers, online safety co-ordinators, LGB members and the IT network manager.

The third section outlines the **Responsibilities of Pupils and Parents** within the Trust schools.

Section 1: Overarching Online Safety Principles and Practise

1.1 Managing Social Networking, Social Media and Personal Publishing Sites

Social Media is a powerful communication tool in today's society and all members of the Trust community are asked to consider what they publish on such platforms carefully. It is advised that members do not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

Concerns regarding a pupil's use of social networking, social media and personal publishing sites (in or out of school) will be raised with the Online Safety Co-ordinator and will be reported to their parents, particularly when concerning the underage use of sites.

Personal use of social networking, social media and personal publishing sites by members of the Trust community will be discussed as part of staff, volunteer and LGB member induction. Generally, staff, volunteers and LGB members should not accept friend requests or other social media invitations from pupils and should not issue such invitations to pupils. Further details are outlined in the Staff/ Volunteer and LGB member Acceptable Use Agreements **(Appendices A and B)** and the Online Communication Code of Conduct which can be (**Appendix C** and Child Protection Policy)**.**

A sample advice leaflet for parents on Social Networking Sites, in particular, Facebook, can be found at **Appendix D.**

Official organisational blogs should be password protected and run from the location website with approval from the Online Safety Co-ordinator. Members of staff are advised not to run social network spaces for pupil use on a personal basis.

In school access to Social Media is restricted for Pupils. 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 headteacher before using Social Media tools in the classroom.

1.2 Use of Digital and Video Images and Webcams

Parental permission will be sought for the use of photographs or video involving their child as part of the agreement when their child joins the school. It is the responsibility of the Online Safety Coordinator to ensure these records are signed and up to date.

The Online Safety Coordinator will also be responsible for ensuring that pupils are not identified in online photographic materials and that full names are not used in any school produced video materials.

If specific pupil photos (not group photos) are used on the Trust/school websites, in the prospectus or in other high profile publications the Online Safety Coordinator will obtain individual parental or pupil permission for its long term use. A model Consent Form can be

found in Kym Allan Health and Safety Consultants Ltd. (KAHSC) General Safety Series G21.

Webcams should be treated like any other type of photography or video, as such parents' wishes around photography of their child should be respected. A risk assessment should be made when using any webcam device and this should be reviewed with the headteacher. Publicly accessible webcams will not be used in school. Webcams will only ever be used for specific learning purposes, i.e. monitoring hens' eggs and never using images of children or adults.

Staff members and volunteers sign the Acceptable Use Agreement (**Appendix A**) at induction and this includes guidance on using digital photographic and video equipment. When making digital images or videos it is recommended that only Trust equipment is used.

Before using digital photographic and video technology with pupils staff must ensure that:

- consent for the use of digital photographs or video involving a pupil or other staff member has been given;
- pupils are not identified in online photographic materials or in any video materials/DVDs produced or published by the Trust/ schools
- they follow Trust procedures concerning the sharing, distribution and publication of those images;
- care is taken to ensure that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the Trust/ school into disrepute.

Images of pupil's work should only be published with the permission of the pupil and parents.

1.3 Managing Mobile Phones and Personal Devices

The use of mobile phones and other personal devices in school or on other Trust premises will be covered in the Acceptable Use Agreements. However, in general the following guidance should be observed by staff, pupils, parents and visitors:

- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the Trust community and any breaches will be dealt with as part of the Trust disciplinary or Whole School Behaviour Policy;
- The Trust reserves the right to search the content of any mobile or handheld devices on the Trust 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;
- Staff may confiscate a phone or device if they believe it is being used to contravene the Whole School Behaviour Policy;
- 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 Bluetooth function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones;
- Electronic devices of all kinds that are brought onto Trust premises are the responsibility of the user. The Trust accepts no responsibility for the loss, theft or damage of such items. Nor will the Trust 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 only during break times. If a staff member is expecting a personal call they may leave

their phone with the school office to answer on their behalf, or seek specific permissions to use their phone at other than their break time;
- Mobile phones and personal devices are not permitted to be used in certain areas within the school site or at certain times such as toilets or within classrooms while pupils are changing.

1.4 Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and the General Data Protection Regulation 2018 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.

Staff, volunteers, LGB members and directors 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.

<u>The use of portable computer systems, USB sticks or any other removable media is prohibited.</u>

More detailed information can be found in the Trust's Data Protection Policy.

1.5 Emailing Personal, Sensitive, Confidential or Classified Information

Emailing confidential data is not recommended and should be avoided where possible. Assess whether the information can be transmitted by other secure means before using email. Where your conclusion is that email must be used to transmit such data ensure that it is sent using the Trust/school's email system.

The following are ways that data can be further protected if sent by email:

- If the main body of the email contains the sensitive information include the word 'confidential' in the subject of the email, this will encrypt the email automatically;

However:

- If attaching a document containing sensitive information it is better to ensure that the document itself is encrypted (password protection). Provide the encryption key or password by a separate email with the recipient;

Take the following precautions to ensure that the information is kept secure:

- Do not identify sensitive information in the subject line of the email;
- Exercise caution 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 telephoning) 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 absolutely necessary.

- Do not send the information to any person whose details you have been unable to separately verify (usually by telephone);
- Request confirmation of safe receipt.

For staff, LGB members and directors and volunteers: The use of Hotmail, BT Internet, G-mail or any other internet based webmail service for sending email containing sensitive information should be avoided wherever possible.

If you have sensitive information that needs to be emailed and you do not use or have access to a Trust/ school based email address then the information should be sent in the first instance to the Head, Chair, Clerk, or other director/LGB member who has access to an email address on the Trust/school system who can follow the procedure outlined above.

1.6 Password Management

NB: The password management process detailed below is considered best practise. The Trust will therefore be working with the network provider and its schools to undertake a process of implementation of this practise through a roll out programme with the aim of compliance across all its sites by September 2019.

1.6.1 Password Setup and Reset:

Currently the management of password security is the responsibility of the network provider. Working with the network provider this responsibility can be shared with locations/ schools, via a password reset tool.

Passwords for new users and replacement passwords for existing users can be allocated by the network provider. An email from the administrator or Online Safety Coordinator must be sent requesting a new password be issued.

If the location has adopted the password reset tool, then the Online Safety Coordinator has the responsibility for managing and setting passwords for new users or replacement passwords for existing users. (this responsibility may be delegated to a Trust/ school administrator, but must be overseen by the Online Safety Coordinator).

1.6.2 Password Security:

The following rules apply to the creation of passwords:

- the last 24 passwords cannot be re-used;
- the password should be at least 12 characters long and must include at least 3 of:
  - uppercase character
  - lowercase character
  - number
  - special character;
- the account will be “locked out” for an hour 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 expire after 12 months, users will receive warnings before their password is due to expire and must choose a new password;
- passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption).

1.7 Incidents of Misuse and Inappropriate Activity

1.7.1 Responding to Incidents of Concern:

Please refer to the Flow Chart at **Appendix E** for how to handle different incidents of misuse and inappropriate activity. Online safety incidents will be managed in accordance

with the Trust Disciplinary or Whole School Behaviour Policy where appropriate. The school will inform parents of any incidents or concerns as and when required.

It is likely that the Trust will need to deal with incidents of inappropriate rather than illegal misuse, however all incidents of inappropriate activity no matter the severity should be reported and handled consistently. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the Trust 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. When responding to any instance of inappropriate activity it is important to refer to:

- Child Protection Policy and Procedures
- Peer on Peer Abuse Policy
- Code of Conduct
- Whole School Behaviour Policy
- Data Protection Policy
- Disciplinary Policy
- Overarching Safeguarding Statement

The Online Safety Coordinator will record all reported incidents and actions taken in any relevant areas e.g. the Online Safety Incident Log **(Appendix F**), 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 Data Protection Officer will be informed of any online safety incidents involving data protection issues, which will then be escalated appropriately as per the Data Protection Policy.

1.7.2 Illegal Activities:

The following activities are unacceptable and illegal and users should not engage in these activities in work/ school or outside work/ school when using Trust equipment or systems to 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;
- extremism or radicalisation of individuals;
- other criminal conduct, activity or materials

Please refer to the Flow Chart at **Appendix E** if any apparent or actual misuse appears to involve illegal activity. 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.

1.7.3 Handling Inappropriate Activities

The Trust believes that the following activities would be inappropriate and users should not engage in these activities in work/school or outside work/school when using Trust equipment or systems:

- visiting Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:
  - 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 Trust or brings the Trust/ school into disrepute;
- running a private business;
- attempting to bypass filtering or other safeguards employed;
- 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.

If instances of such behaviour are discovered or suspected, where 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. If technical support is required to conduct the investigation please contact the Network Manager.

After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required and inform the Trust if they believe that there are implications across the whole Trust.

If at any time there is uncertainty about how to proceed with any incidents of concern, then the incident may be escalated to the Safeguarding Hub – see Child Protection Policy and Procedures.

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

1.8. Managing Cyber-bullying

Cyber-bullying (along with all other forms of bullying) of any member of the Trust community will not be tolerated. Further advice can be found in the Peer on Peer Abuse Policy.

When dealing with incidents of Cyber-bullying the school will:

- record all incidents of cyber-bullying reported;
- advise pupils, staff and parents to keep a record of the bullying as evidence;
- take steps to identify the bully, where possible and appropriate;
- inform parents of pupils
- contact the Police if a criminal offence is suspected
- follow safeguarding procedures as outlined in the Child Protection Policy and Procedures as appropriate

Sanctions for those involved in cyber-bullying will follow the Whole School Behaviour Policy, Acceptable Use Agreement and Disciplinary Procedures.
They may also include:

- asking the bully to remove any material deemed to be inappropriate or offensive;
- contacting a service provider to remove content if the bully refuses or is unable to delete content.

Section 2: Roles and Responsibilities

The following section outlines the roles and responsibilities for online safety of individuals and groups within the Trust community:

2.1 Directors & Officers

2.1.1 Trust Data Protection Officer and Safeguarding Director

The Trust, through the Data Protection Officer, will take overall responsibility for data and data security. The Data Protection Officer will handle all instances of data breach as per the Data Protection Policy.

Safeguarding incidents reported to the Safeguarding Director will be handled in line with the Child Protection Policy and Procedures and Overarching Safeguarding Statement.

2.1.2 Trust Board of Directors

The Trust directors can appoint a member with responsibility for online safety, if you prefer this role could be combined with the director with responsibility for safeguarding.

The Board of Directors will:

- ensure that the Trust schools and the central Trust staff follow all current online safety advice to keep children and staff safe;
- monitor online safety by receiving regular information about online safety incidents;
- work with the Online Safety Coordinator in each school to maintain and overview of the incident logs
- support its schools in encouraging parents and the wider community to become engaged in online safety activities;

When visiting or working in school or at the central Trust premises directors must:

- act reasonably taking into account the needs of other users e.g. the downloading of large files during the working day will affect the service that others receive;
- take responsibility for their network use;
- ensure that personal/Trust data sent over the Internet or taken off site is encrypted. (See section 1.5 on Emailing Personal, Sensitive, Confidential or Classified Information);
- not use portable media e.g. USB thumb drives, portable hard discs etc. to transfer information;
- not install or send as an email attachment *any unapproved software;*
- ensure as far as possible in your role that access to personal data is securely controlled in line with the Trust's Data Protection Procedures.

2.1.3 Managing Your Account and Email as a Trust director

It is a requirement that the Chair of the Trust and the Chair of each standing committee operates a Trust email account for all Trust business. It is further recommended that each director uses a Trust based email account for all Trust business. Where this is not the case directors must ensure that the email address they use is not a shared account, accessible by individuals not directly engaged in the Trust business.

Directors with a Trust email address will have responsibility for the security of their username and password. These must not be shared and breaches or evidence that there has been a breach must be immediately reported to the Data Protection Officer and the Network Manager.

The directors will maintain on overview of the online safety audit (**Appendix G**) work undertaken at each location to establish if the Online Safety Policy and Procedures are working effectively and being implemented. Methods to identify, assess and minimise risks will be reviewed regularly.

2.2 Local Governing Bodies (LGB's)

The LGB in each school can appoint a member with responsibility for online safety, if you prefer this role could be combined with the LGB member with responsibility for safeguarding.

The LGB will:

- ensure that the school follows all current online safety advice to keep children and staff safe;
- monitor online safety by receiving regular information about online safety incidents;
- undertake reviews of incident logs, filtering/change control logs etc. with the Online Safety Coordinator;
- sign the Acceptable Use Agreement for LGB members (**Appendix B)** on induction to the LGB and engage in training to maintain understanding of current online safety issues;
- support the school in encouraging parents and the wider community to become engaged in online safety activities;

When visiting or working in school LGB members must:

- act reasonably taking into account the needs of other users e.g. the downloading of large files during the working day will affect the service that others receive;
- take responsibility for their network use;
- ensure that personal/school data sent over the Internet or taken off site is encrypted. (See Emailing Personal, Sensitive, Confidential or Classified Information section 10);
- not use portable media e.g. USB thumb drives, portable hard discs etc. to transfer information to and from school;
- not install or send as an email attachment *any unapproved software;*
- ensure as far as possible in your role that access to personal data is securely controlled in line with the Trust's Data Protection procedures.

2.2.1 Managing Your Account and Email as an LGB Member

It is a requirement that the Chair of each school LGB operate a school based email account for all LGB business. It is further recommended that each LGB member uses a school based email account for all LGB business. Where this is not the case LGB members must ensure that the email address they use is not a shared account, accessible by individuals not directly engaged in the LGB business. The setting up of school based email accounts can be arranged by the headteacher and school administrator

LGB members with a school based email address will have responsibility for the security of their username and password. These must not be shared and breaches or evidence that there has been a breach must be immediately reported to the school's Online Safety Co-ordinator and the Network Manager.

Users must immediately report, to the Online Safety Co-ordinator, 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.

2.2.2 Assessing Risks

The LGB member with responsibility for online safety will work with the headteacher (and the schools Online Safety Coordinator) to audit ICT use to establish if the Online Safety Policy and Procedures are being implemented – see **Appendix G** for the Online Safety Audit.

2.3 Online Safety Responsibility - Role of the Online Safety Coordinator

For the purposes of this document the Online Safety Coordinator is the individual either directly or by delegation that takes on responsibility for online safety.

The headteacher/ Executive headteacher has overall responsibility for online safety provision in each of their designated Trust schools. The day to day responsibility for online safety, or elements of the role, may be delegated.

For central Trust operations the responsibility for online safety provision rests with the CEO. The day to day responsibility for online safety, or elements of the role may be delegated, for central Trust operations.

In whichever way the Online Safety Coordinator responsibilities are organised the individual delivering the Online Safety Coordinator role will:

- take responsibility for data and data security on a day to day basis and will report data breaches to the Data Protection Officer, see the Data Protection Policy;
- review the users of the Trust/ school information systems regularly and maintain a current record of all directors, LGB members, volunteers, staff and pupils who are granted access to the electronic communications;
- provide, at induction for all new staff (including those on university/college placements and work experience) volunteers, directors and LGB members, information and guidance on the Online Safety Policy and Procedures and the Acceptable Use Agreements and Online Code of Conduct **(Appendix A,B and C).**
- ensure that they and other relevant staff receive suitable CPD to enable them to carry out their online safety roles and to train other colleagues, as relevant;
- ensure that adequate CPD opportunities are available to all staff to ensure that they remain aware of all online safety developments;
- log online safety incidents and ensure such a log (**Appendix F**) is kept up to date;
- be aware of the procedures to be followed in the event of a serious online safety incident or an allegation being made against a member of staff or volunteer (see flow chart on dealing with online safety incidents – (**Appendix E)**, and relevant safeguarding, capability/disciplinary procedures). The procedures for dealing with allegations against staff or volunteers can be found within the Trust's Child Protection Policy and all staff/ volunteers are provided with a copy on induction;
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident or allegation against a member of staff or volunteer;
- if the role is delegated - communicate regularly with the headteacher/ CEO regarding all online safety monitoring and issues;
- where other staff members have monitoring responsibilities have a system in place to allow for monitoring and support of these individuals to provide a safety net and support to those colleagues who take on important monitoring roles;
- liaise with ICT technical staff and the Network Manager
- embed an awareness and commitment to online safety throughout the Trust community and across the curriculum;
- communicate regularly with the designated online safety Director/ LGB member/committee to discuss current issues, review incident logs (**Appendix F**) and filtering/change requests, and complete the Online Safety Audit (**Appendix G**);
- have an awareness of emerging online safety issues and legislation, and of the potential for serious child protection issues which could arise from:
    - the 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

As part of the commitment to online safety, the Trust schools should operate a rolling programme of advice, guidance and training for parents, which could include but not be limited to:

- the provision of information leaflets, articles in the school newsletter or 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

2.3.1 User IDs and Security

The Online Safety Coordinator will ensure that the location in which they work has full records of:

- User IDs and requests for password changes;
- 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.

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 the headteacher/ CEO (and if delegated with the Online Safety Coordinator) at least annually to ensure that they are up to date and will ensure that old users are removed as soon as possible. This will prevent the growth of Zombie Accounts.

Zombie accounts refer to accounts belonging to users who have left and therefore no longer have authorised access to the IT systems. Such Zombie accounts when left active can cause a security threat by allowing unauthorised access. To prevent such security breaches:

- Ensure that all user accounts are disabled once the user has left;
- Prompt action on disabling accounts will prevent unauthorised access;

2.3.2 System Back Ups

If the location has chosen to take this task in-house it is the responsibility of the Online Safety Coordinator to check the daily email confirmation of a successful back up. If the email reports any problem with the back up this must be reported immediately to the Network Manager. Failure to report problems could leave the IT system vulnerable in the event of a system failure.

2.3.3 Managing Published Content

For further information about website compliance please refer to the Website Compliance checklist and the Data Protection Policy.

It is the responsibility of the Online Safety Coordinator to review the school website regularly to check for compliance and to organise updates as necessary.

The headteacher/ CEO will retain overall editorial responsibility for online content published by the school/ Trust and will ensure that content published is accurate and appropriate. Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Each website will contain the Trust's Privacy Policy, the Trust's logo and Company Number and for schools a page giving a brief introduction to the Trust. This page will link to the central Trust website.

2.3.4 CCTV

Where Trust schools use CCTV for security and safety the headteacher retains overall responsibility, but may give named individuals access to it. A log of the named individuals given access to the CCTV must be kept, monitored and managed.

2.3.5 Managing Filtering

Filtering for Trust schools is currently provided by Cumbria ISP and it is up to the Online Safety Coordinator to work with them to ensure that filtering is working effectively (school.ictsupport@cumbria.gov.uk; 01228 221225).

The Online Safety Coordinator will ensure:

- The school has a clear procedure for reporting breaches of filtering and that all members of the school community (all staff and all pupils) are aware of this procedure:
    - *If staff or pupils discover unsuitable sites, the URL will be reported to the Online Safety Coordinator who will then record the incident and escalate the concern as appropriate;*
- that changes to the school filtering procedures are risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the headteacher.
- that regular checks are arranged and undertaken to ensure that the filtering methods selected are effective;
- that any material that the school believes is illegal will be reported to appropriate agencies such as the Police, the Internet Watch Foundation or the Child Exploitation and Online Protection command;
- the school's access strategy is suitable for the age and curriculum requirements of the pupils, with advice from Cumbria ISP or the Network Manager as appropriate.

2.3.6 Managing Emerging Technologies

The headteacher will examine and evaluate emerging technologies for educational benefit. A risk assessment will be carried out before use is allowed.

2.3.7 Managing ICT Equipment and Disposal

The Online Safety Coordinator will maintain a comprehensive inventory of all ICT equipment using the Asset Register and will be responsible for organising secure disposal of equipment.

The Network Manager will take on the disposal work at the request of the headteacher. However it is the responsibility of the Online Safety Coordinator to inform the Network Manager if personal data is likely to be held and for making a disposal record in the Asset Register which 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

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.

If the Network Manager (or any other supplier) has been asked to arrange disposal of redundant ICT Equipment then they should be asked to quote for this work using the following criteria:

- ensure that any disposal carried out professionally and to the best of their knowledge fulfils statutory requirements and regulations;
- keep confirmation of secure disposal where applicable.
- explore options for reusing equipment (rather than landfill) that supports the charitable aims of the Trust.

2.4 Network Manager

The Network Manager will:

- ensure that users only access the locations IT networks through an authorised password protection procedure, in which passwords are changed after no longer than 12 months;
- ensure as far as possible that the location's ICT infrastructure is secure and is not open to misuse or malicious attack;
- maintain a firewall that allows access to the internet which utilises the web filtering provided at each location.
- Ensure that unrestricted access to the internet is not available unless pre-approved by the headteacher/ CEO for specific staff members or for a specific purpose;
- ensure that access controls/encryption exist to protect personal and sensitive information held;
- keep up to date with the Online Safety Policy and Procedures and technical information in order to effectively carry out their online safety role;
- ensure that appropriate backup monitoring procedures are available to each location. Where the location has given the Network Manager this responsibility, they will monitor the back-up procedure every day and make any necessary changes to ensure that critical information and systems can be recovered in the event of a disaster and in order to complement the business continuity process. If the location has chosen to monitor this themselves it will be the responsibility of the Online Safety Coordinator (see page 4 above);
- keep up-to-date documentation of the location's e-security & technical procedures.
- Hold the "master/administrator" passwords for each location's ICT system

2.4.1 Maintaining Information Systems Security

To maintain Local Area Network (LAN) security the Network Manager will:

- Ensure workstations are, as far as possible, secured against user mistakes and deliberate actions.
- Ensure that servers are located securely and physical access restricted.
- Keep the server operating system secured and up to date.
- Manage access by wireless devices with a minimum of WPA2 encryption.

2.4.2 User Accounts

The Network Manager will be responsible for ensuring that the location's IT 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;

A safe and secure username/password system is essential if the above is to be established and will apply to all Trust ICT systems. The Network manager will therefore work with each location in the management of password security.

Pupil's email addresses will be set up to block the sending or receiving of emails from outside the school's own email domain. A forwarding block will be also put on all accounts to prevent fraudulent use.

2.4.3 Assessing Risks

The Network Manager alongside the Trust, and it's 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 Trust computer. Liability cannot be accepted by the Network Manager or the Trust for the material accessed, or any consequences resulting from internet use. However the Network Manager will ensure that methods to identity, assess and minimise risks are reviewed regularly and will bring to the Trusts attention any improvements that could be implemented.

2.5 All Staff

It is the responsibility of **all** staff to:

- read, understand and help promote the Trust's Online Safety Policy & Procedures;
- read, understand & adhere to the Staff Acceptable Use Agreement (**Appendix A**);
- be aware of online safety issues related to the use of mobile phones, cameras and hand-held devices and to monitor their use and implement current procedures with regard to these devices;
- report any suspected misuse or problem to the Online Safety Coordinator
- maintain an awareness of current online safety issues and guidance e.g. through CPD opportunities;
- model safe, responsible and professional behaviours in their own use of technology;
- act reasonably whilst using ICT equipment during the work day e.g. being aware that the downloading of large files during the working day will affect the service that others receive.
- take responsibility for their network use.
- ensure that personal data sent over the internet is encrypted
- not use portable media e.g. USB thumb drives, portable hard discs etc. to transfer information to and from school;
- ensure that unapproved software is not used in work areas or attached to email.

2.5.1 Teaching Staff

Members of staff with teaching duties have additional responsibilities, they must:

- ensure that online safety issues are embedded in all aspects of the curriculum and other school activities;
- monitor, supervise and guide pupils carefully when engaged in ICT activity in lessons, extra-curricular and extended school activities;
- ensure that pupils are fully aware of research skills and are made aware of legal issues relating to electronic content such as copyright laws as appropriate;
- ensure that during lessons where internet use is pre-planned pupils are guided to sites checked as suitable for their use;
- ensure that processes are known and used when dealing with any unsuitable material that is found in internet searches;
- plan Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas;
- consider how to ensure access to technology and the curriculum is managed for vulnerable members of the school community (such as with children with special education needs) staff should make decisions based on the specific needs and understanding of the pupil(s).
- introduce pupils to their responsibilities through the Acceptable Use Agreement (**Appendix H**);
- Ensure that pupils understand the issues around:
    - email safety, such as the risks attached to the use of personal details and dealing with inappropriate emails;
    - aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying online, online gaming/gambling etc.

When using digital images and digital imaging technology with pupils, staff should inform and educate pupils (in an age appropriate way) about:

- risks associated with the taking, use, sharing, publication and distribution of images.
- how images can be manipulated;
- the importance of consent when publishing on the internet
- the risks associated with providing information with images that reveals the identity of others and their location, such as house number, street name or school.

2.5.2 Managing Your User Account

Each staff member will have their own user account. All users (staff or volunteer) will have responsibility for the security of their username and password, and must not allow other users to access the systems using their log on details. Any suspicion or evidence that there has been a breach must be immediately reported to the Online Safety Coordinator.

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

- at induction through the Acceptable Use Agreement.
- through the Online Safety Policy and Procedures.

2.5.3 Managing Email and Communications

Staff will only use their official school provided email accounts to communicate with pupils, parents and for all professional purposes. It is the responsibility of every staff member to maintain the security of their username and password.

The following key points about email & communications should be adhered to at all times:

- Personal email addresses, text messaging or public chat/social networking programmes must not be used for communications with pupils or parents in your professional capacity;
- Any digital communication between staff and pupils or parents (email, chat etc.) must be professional in tone and content;
- Email sent to external organisations should be written carefully, in the same way as a letter written on school headed paper would be;
- The official school email service may be regarded as safe and secure. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access);
- Users must immediately report, to the Online Safety Coordinator, 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;

2.5.4 Training

Staff will take up any opportunity to enhance their understanding of online safety issues through training appropriate to their role.

2.5.5 Managing Filtering

Staff should be aware of the procedure for reporting failures in the internet filtering and understand that changes to the filtering can be requested for specific educational purposes. Staff should:

- Report the discovery of unsuitable sites to the Online Safety Coordinator as soon as possible
- risk assess, with help from staff members with technical experience if possible, any sites they wish to use that are currently blocked by filtering. The risk assessment should then be discussed with the headteacher before requesting a change;
- report any material that they believe is illegal to the Police, the Internet Watch Federation or CEOP as soon as possible as well as the Online Safety Coordinator.

2.5.6 Staff Use of Personal Devices

Members of staff, volunteers and others working in school 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. Furthermore:

- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and only use work-provided equipment for this purpose;
- Where members of staff are asked to use a mobile phone for school duties or in an emergency where a staff member does not have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

Section 3: Responsibilities of Pupils and Parents

3.1 Pupils

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

- use the school ICT systems in accordance with the Pupil Acceptable Use Agreement (**Appendix H**), which they and/or their parents will be expected to sign before being given access to school systems; (NB. at EYFS and KS1 it would be expected that parents would sign on behalf of the pupils)
- know and understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- know what action to take if they or someone they know feels worried or vulnerable when using online technology;
- know and understand school procedures on the use of mobile phones, digital cameras and hand-held devices;
- know and understand school procedures on the taking/use of images and on cyber-bullying;
- understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy and procedures covers their actions out of school, if related to their membership of the school;
- take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home;
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

3.1.1 Managing Accounts

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

- in ICT and/or online safety lessons
- through the Acceptable Use Agreement

If pupils are given usernames and passwords they should understand the importance of keeping these safe, keeping them secret and what to do if they think there is a problem. If the school uses whole class log-ons the same messages should be shared and adapted to suit the age and ability of the pupils.

3.1.2 Managing Email

In Primary School: If pupils have access to an email account within school it will be set up so that it cannot receive email from outside the school system and can only send email to an address within the school system, this will be managed by the Network Manager.

For communication outside school a whole class or group email will be used and managed by a member of staff.

When using email within school pupils should understand that they:

- may only use approved email accounts for school purposes;
- must immediately tell a member of staff if they receive an offensive email or one which upsets or worries them and that they should not respond to it;
- must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.

3.1.3 Social Media

Pupils should understand that excessive social email use can interfere with learning and access to social media is restricted within school.

3.1.4 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 headteacher 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. Mobile phones and devices will be released only to a responsible adult;
- Phones and devices must not be taken into examinations. Pupils found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the pupil's withdrawal from either that examination or all examinations;
- If a pupil needs to contact his/her parents they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.

3.2 Parents

Parents play a crucial role in ensuring that their children understand the need to use the online technology and devices in an appropriate way. 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 where the pupil themselves cannot sign – see **Appendix H**;
- access the school website or other online system 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;
- 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.

3.2.1 Training Opportunities

Parents should be made aware of the school's programme of advice, guidance and training. Parents should take advantage of these opportunities to ensure that they have a full understanding of this constantly changing area and are best able to support their children. There is a list of useful online safety links at **Appendix I**.

3.2.2 Use of Digital Photographs, Video and Webcams

Parents should ensure that they read and understand the photographic consent form they sign for their child. If at any time parents wish to change their consent they should inform the school immediately.

3.2.3 CCTV

Notification of CCTV use is displayed at the front of the school/ Trust premises. Please refer to the Information Commissioners Office (ICO) for further guidance. For questions or concerns regarding CCTV please contact the headteacher.

3.2.4 Complaints

The Trust 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 Trust computer or mobile device. Neither the Trust staff nor the

Local Governing Body or Trust Board of Directors can accept liability for material accessed, or any consequences of Internet access.

- Complaints about the misuse of online systems will be dealt with under the Trust's Complaints Procedure;
- Complaints about cyberbullying will be dealt with in accordance with the Whole School Behaviour Policy and the school's own bullying procedures;
- Complaints related to child protection are dealt with in accordance with the Child Protection Policy and Procedures;
- Any complaints about staff misuse will be referred to the headteacher or to the Chair of the LGB if the complaint concerns the headteacher;
- All online safety complaints and incidents will be recorded by the individual schools including any actions taken (see **Appendix F**).

Appendix A

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 **NAME OF PERSON** (Online Safety Coordinator) or **NAME OF PERSON** (Headteacher).

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 will only use my own user name and passwords which I will choose carefully so they cannot be guessed easily. I will also change the passwords after a 12 month period, when I am prompted.
- 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 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 LGB member 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 Trust Data Protection Policy. 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 headteacher or Local Governing Body. Personal or sensitive data taken off site in an electronic format must be encrypted, e.g. on a password secured laptop. Staff members 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 Trust's Online Safety, Data Protection and the Whole School 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 curriculum.
- 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 and any related technologies for professional purposes or for uses deemed 'acceptable' by the headteacher, Online Safety Coordinator or Local Governing Body.
- I will communicate online 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 online 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 LGB member.
- I will not use personal email addresses on the school ICT systems.

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 online 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 headteacher 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 Trust 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 Trust community.

Buying/Selling/Gaming

- I will not use Trust 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 headteacher.
- I will not install any hardware of software on a computer or other device without permission of the Network Manager.
- I will not try to alter computer settings without the permission of the Network Manager.
- I will not cause damage to ICT equipment.
- 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 LGB members / 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 It 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 the ICT systems at my place of work or at home when I have permission to do so
- ✓ I use my own ICT (where permitted) in my place of work
- ✓ I use my own ICT out of work to access for activities relating to my employment by the Trust

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

Appendix B

LOCAL GOVERNING BODY MEMBER ACCEPTABLE USE AGREEMENT

This Agreement is designed to ensure that all LGB members 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 LGB members role in the school. All LGB members (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 **NAME OF PERSON** (Online Safety Coordinator) or **NAME OF PERSON** (Headteacher).

This Acceptable Use Agreement is intended to ensure that:

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

School networked resources are intended for educational purposes and may only be used for legal activities consistent with the rules of the Trust and school. If you make a comment about the Trust or School, 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 or Trust 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.
- LGB members 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 Headteacher /Chair of LGB

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 name and passwords which I will choose carefully so they cannot be guessed easily. I will also change the passwords when prompted at the end of 12 months, 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 headteacher 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 LGB member 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 Trust'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 or Trust 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 headteacher. 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 ScholarPack.
- 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 headteacher 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.

✂ ----------

LGB Member 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 headteacher.

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 LGB members under reasonable suspicion of misuse in terms of access or content may be placed under retrospective investigation or have their usage monitored.

LGB Member Name			
Signed		**Date:**	

Appendix C

Online Communication Code of Conduct for Staff Working with Children

Rationale and context:
Over the past years the use of blogs, chat rooms and social networking sites, such as Twitter and Facebook has become increasingly popular. Such sites are used to chat with and share information, photographs and news with friends across the world.

Whilst the use of such sites has very many benefits there are potential problems concerning privacy and inappropriate usage. These may include breaches of confidentiality, unsuitable language or images, and in some cases breaches of the law.

Examples of such problematic usage of publicly accessible social networking could be:

- Staff referring to parents or children and young people by name
- Staff referring to forthcoming trips/visits
- Staff using derogatory or offensive language about parents, colleagues, managers, or the organisation for which they work.
- Staff posting images of themselves in inappropriate dress or situations
- Staff participating in illegal activities such as the sharing of indecent images of children
- Partners or friends posting inappropriate comments concerning staff
- Partners and friends posting images that show staff members in situations which may not be in keeping with their professional status

This code of conduct is designed to protect staff who may use such sites in their private lives. It must be recognised that those who work with children have a duty to demonstrate the highest standards of conduct or integrity and make sure that their actions in their private lives do not put themselves in a situation when their conduct or integrity might be called into question or potentially bring their employer into disrepute. This could result in disciplinary action by your employer or even criminal prosecution. This code of conduct sets out expectations around online behaviour that could affect professional standing, integrity and dignity.

What this code does not cover:

- Social contact between adult colleagues. However, staff need to be mindful of what they are posting and who can see it. This is important in respect of confidentiality, workplace relationships, and the fact that their online contacts may not appreciate the difference between private and professional comments.
- Membership of professional networks or forums is not covered by this code as these are usually covered by a professional body's own code of conduct.

Membership of forums is not covered, although in extreme cases legal restrictions may apply. Staff should however remember that what they say may reflect upon their professional lives and moderate their comments accordingly.

Code of Conduct:

- Staff should not allow themselves to enter into online contact with children they work with, parents or their families. Friend requests from parents or children and young people under the age of 18 (past or present) in this context should be politely declined by explaining that it is against agency policy, which is designed to protect staff from abuse and misunderstandings.
- Staff should not create web pages, groups or contact lists concerning professional activities carried out on behalf of their agency unless they have express written permission from a senior manager to do so.
- There must be absolutely no private online contact between staff and any children and young people with whom they have a work-related relationship. This includes the storing of images of children under the age of 18.
- Any contact with children and young persons after they have left the organisation (e.g. moved to a secondary school) should be sanctioned by a senior manager within the organisation and the parent and not occur through social networking sites or other online communication technologies
- Online contact made as part of professional duties should always be carried out using technologies provided by the agency or local authority. These technologies should have the capability of logging and storing records securely.
- Staff are strongly advised to be careful about what they say online in contact with other young people such as relatives or family friends. This caution should apply to images or video material.

Staff privacy and dignity

Staff are strongly recommended to check that their online privacy settings only allow "friends" to see their profiles. It is also advised that staff do not accept friend requests from people who are not personally known to them.

Staff may wish to ask friends to check before photographs are posted which may cause them embarrassment. Staff posting their own images should bear in mind the fact that any image can easily be downloaded and manipulated and they should choose which images they share accordingly.

It is recommended that staff do not post images that could be used to identify their homes or families.

All staff are advised to make themselves familiar with the parent pages on the CEOP "Think You Know" site at www.thinkyouknow.co.uk and keep themselves up to date with the risks of emerging technologies.

The Link with the 'Guidance for Safer Working Practice for adults who work with children and young people'

This document is endorsed by the Cumbria local safeguarding children's board (LSCB) and is being adopted by organisations that employ staff to work with children throughout Cumbria. Section 12 of the guidance covers communication with children and young people using (including the use of technology). This states that:
'Communication between children and adults by whatever method should take place within clear and explicit professional boundaries'.

Specifically the guidance recommends that adults should;

- Not give their personal contact details to children and young people including their mobile telephone number and details of any blogs or personal websites
- Only use equipment e.g. mobile phones, provided by the organisation to communicate with children and young people, making sure their parents have given permission for this form of communication to be used.
- Only make contact with children for professional reasons and in accordance with any organisational policy.
- Recognise that text messaging is rarely an appropriate response to a child in crisis or at risk of harm. It should only be used as a last resort where other forms of communication are not possible.
- Not use internet or web-based communication channels to send personal messages to a child/young person.

Ensure that if a social networking site is used, details are not shared with children and young people and privacy settings are set at maximum.

Appendix D

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.

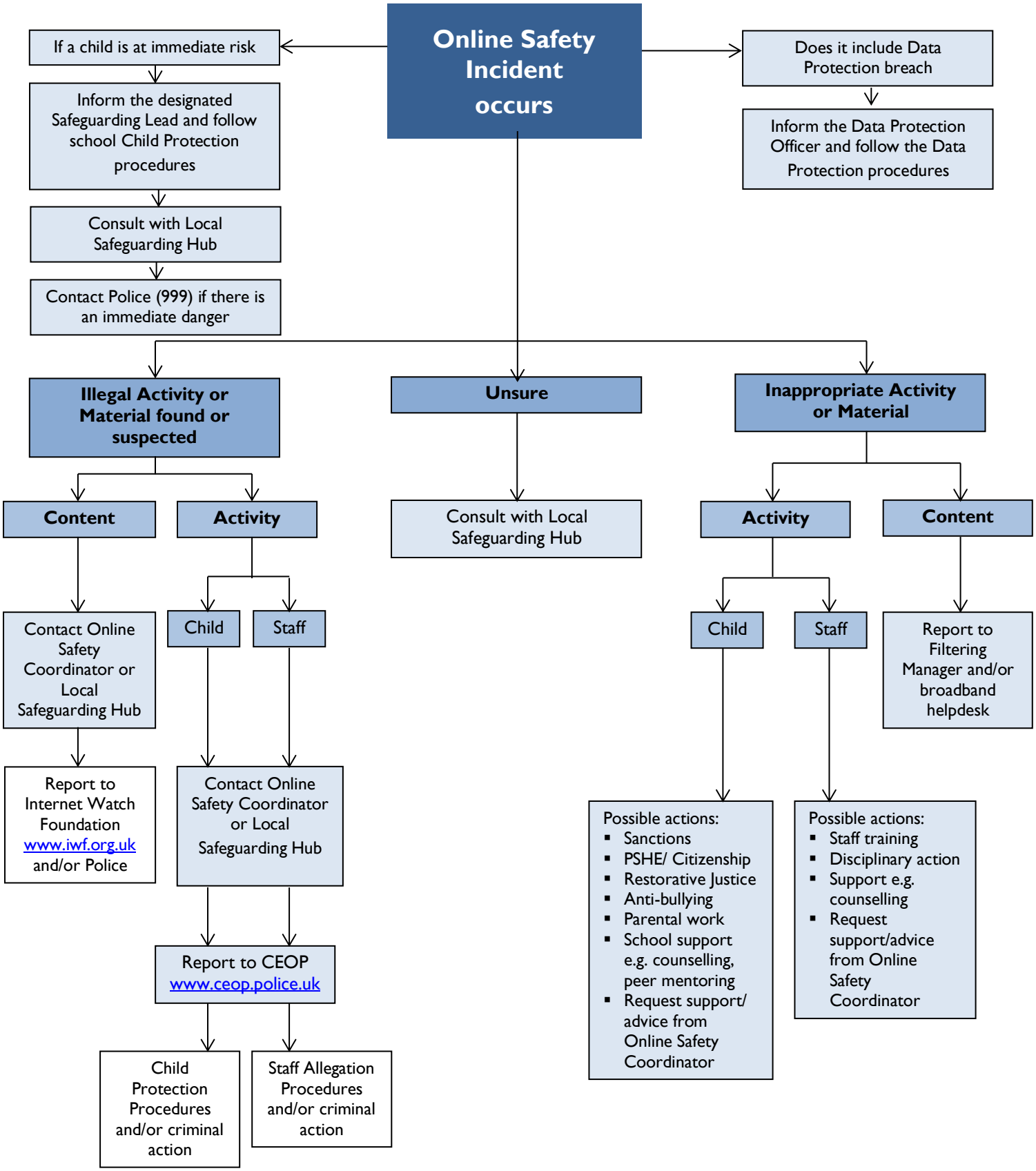
Should you decide to allow your children to have a Facebook profile we strongly advise you to:

- 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.

RESPONSE TO AN INCIDENT OF CONCERN



Review Online Safety Policy and Procedures; record actions in Online Safety Incident Log and implement any changes in the future. Contact the Trust if it is felt athat the review will have benefits across the Trust.

Good Shepherd Trust

ONLINE SAFETY INCIDENT LOG

YOUR LOGO HERE

Details of Online Safety incidents are to be recorded by the headteacher or Online Safety Coordinator. This incident log will be monitored termly by the headteacher and LGB member with responsibility for online safety.

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

Appendix G

XXXX SCHOOL ONLINE SAFETY AUDIT

This self-audit should be completed by the headteacher or Online Safety Coordinator or other member of the Senior Leadership team as delegated. Staff that could contribute to the audit include: Designated Safeguarding Lead, SENCO, Online Safety Coordinator, Network Manager and LGB member with responsibility for safeguarding or online safety.

The Online Safety Policy and procedures is available for staff to access at:	
The Online Safety Policy and procedures is available for parents to access at:	
The LGB member responsible for Online Safety is:	
The Designated Safeguarding Lead is:	
The Online Safety Coordinator is:	

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 expectations 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**
Is personal data collected, stored and used according to the principles of the Data Protection Act and the Trust's Data Protection Policy?	**YES / NO**
Are members of staff with responsibility for managing filtering, network access and monitoring systems adequately supervised?	**YES / NO**
Does the online safety co-ordinator log and record all incidents, including any action taken?	**YES / NO**
Are the Local Governing Body and headteacher/ Online Safety Coordinator monitoring against the Online Safety Policy and Procedures on a regular basis?	**YES / NO**

Appendix H

PUPIL ACCEPTABLE USE AGREEMENT
(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 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 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 ICT systems and email can be checked and my parent contacted if a member of staff is concerned about my safety.
- I will not sign up for any online service unless this is an agreed part of a project approved by my teacher.

✂----------

PUPIL and PARENT
ACCEPTABLE USE AGREEMENT

Dear Parent(s),

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 **Name of Person.**

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

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 **XXXX** School.

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

Appendix I

ONLINE SAFETY LINKS

The following links may help those who are developing or reviewing Online Safety Policy and Procedures or want further information.

- **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. 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