CLEATOR MOOR NURSERY SCHOOL

ONLINE SAFETY POLICY & PROCEDURES

Approved by	
Name:	Lisa Wilson and Tracey Lightfoot
Position:	Headteacher and Chair of Governors
Signed:	
Date:	January 2018
Review date:	January 2021

[1] The Governing Body are free to delegate approval of this document to a Committee of the Governing Body, an individual Governor or the Head Teacher.
[2] Governors free to determine review period.

REVIEW SHEET

The information in the table below details earlier versions of this document with a brief description of each review and how to distinguish amendments made since the previous version date (if any).

Version Number	Version Description	Date of Revision
1	Original	February 2012
2	Front Cover ONLY updated to take account of revised Statutory Policy Guidance issued by the DfE	March 2013
3	Minor changes to reinforce the need for parents to act responsibly when using Facebook or other social networking sites	November 2013
4	Reformatted only	April 2014
5	Amended to include references to extremism, radicalisation and child sexual exploitation and minor changes to text	September 2015
6	Updated to remove statutory references to home-school agreement, change of title to 'Online Safety Policy and procedures' in line with Ofsted terminology and the document split into Policy and Procedures	March 2016
7	Updated to reflect changes as a result of updated 'Keeping Children Safe in Education' – September 2016	August 2016
8	Minor changes/ updated	January 2018

Contents

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

Appendix A - School Online Safety Audit

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

Appendix C - Response to an Incident or Concern Flow Chart

Appendix D - Sample Online Safety Incident Log

Appendix E - Online Safety Links

Appendix F - Legal Framework

Appendix G - Glossary of Terms

POLICY

1. Background/Rationale

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

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

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

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

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

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

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

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

2. Definitions

For the purposes of this document a child, young person, pupil or student is referred to as a 'child' or a 'pupil' and they are normally under 18 years of age.

Wherever the term 'parent' is used this includes any person with parental authority over the child concerned e.g. carers, legal guardians etc.

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

Wherever the term 'school' is used this also refers to Governing Bodies and will usually include wrap around care provided by a setting.

3. Associated School Policies and procedures

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

- Overarching Safeguarding Statement
- Child Protection Policy and procedures
- Data Protection Policy including procedures for CCTV
- Health and Safety Policy and procedures
- Whole School Behaviour Policy
- Procedures for Using Pupils Images
- Code of Conduct for staff and other adults
- E-Safety Information Policy (for parents/ carers)
- ICT Acceptable Use Policy
- ICT Mobile Phone Policy
- Parental Use of Social Networking and Internet Sites

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

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

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

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

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

5. Schedule for Development / Monitoring / Review

This Online Safety Policy and procedures was approved by the *Governing Body/Governing Body Committee on:*	*15th March 2018*
The implementation of this Online Safety Policy and procedures will be monitored by the:	*Headteacher – Lisa Wilson*
Monitoring will take place at regular intervals:	*Annual monitoring with 3 yearly full review*
The *Governing Body/Governing Body Committee* will receive a report on the implementation of the Online Safety Policy and procedures generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	*First full GB meeting of the year*
The Online Safety Policy and procedures will be reviewed in accordance with the Governors decision on frequency, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	*January 2018*
Should serious Online safety incidents take place, the following external persons/agencies will be informed:	*LA ICT Manager, DO, Police, Information Commissioner's Office, Safeguarding Hub (if appropriate)*

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

- *Logs of reported incidents*
- *Internal monitoring data for network activity*

6. Scope of the Policy

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

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the School site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online safety related incidents covered by this Policy and procedures, which may take place out of school, but is linked to membership of the School. The 2011 Education Act increased these powers with regard to the searching for, and of, electronic devices and the deletion of data. In the case of both acts, action can only be taken with regard to issues covered by the published Whole School Behaviour Policy.

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

PROCEDURES

1. Roles and Responsibilities

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

1.1 Governors

The role of the Governors is to:

- ensure that the school follows all current online safety advice to keep the children and staff safe;
- approve the Online Safety Policy and procedures and review its effectiveness. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor
- support the school in encouraging parents and the wider community to become engaged in online safety activities;
- regular review with the Headteacher

1.2 Headteacher

The Headteacher has overall responsibility for online safety provision. The day to day responsibility for online safety may be delegated to the Senior Teacher.

The Headteacher will:

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

1.3 Online Safety Coordinator/Designated Safeguarding Lead

The Designated Safeguarding Lead will:

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

- potential or actual incidents of grooming
- cyberbullying and the use of social media

1.4 Network Manager/Technical staff

The External ICT Support Company:

- report any online safety related issues that arise, to the Headteacher;
- ensure that users may only access the school's networks through an authorised and properly enforced password protection procedures, in which passwords are regularly changed;
- ensure that the school's ICT infrastructure is secure and is not open to misuse or malicious attack e.g. keeping virus protection up to date;
- that the school meets the online safety technical requirements outlined in the School Acceptable Use Agreements and any relevant Local Authority Online Safety Policy and guidance;
- the school's procedures on web filtering, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person;
- ensure that access controls/encryption exist to protect personal and sensitive information held on school-owned devices;
- that he/she keeps up to date with the school's Online Safety Policy and procedures and technical information in order to effectively carry out their Online safety role and to inform and update others as relevant;
- ensure that appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster and in order to complement the business continuity process;
- keep up-to-date documentation of the school's e-security and technical procedures.

1.5 All Staff

It is the responsibility of all staff to:

- read, understand and help promote the school's Online Safety Policy and procedures
- read, understand and adhere to the school Staff Acceptable Use Agreement;
- be aware of online safety issues related to the use of mobile phones, cameras and hand-held devices and that they monitor their use and implement current school procedures with regard to these devices;
- report any suspected misuse or problem to the Online Safety Coordinator / Headteacher;
- maintain an awareness of current online safety issues and guidance e.g. through CPD opportunities;
- model safe, responsible and professional behaviours in their own use of technology;
- ensure that any digital communications with pupils are on a professional level and only through school-based systems, never through personal mechanisms, e.g. email, text, mobile phones or social media messaging or posts.

Teachers must:

- ensure that online safety issues are embedded in all aspects of the curriculum and other school activities;
- monitor, supervise and guide pupils carefully when engaged in ICT activity in lessons, extra-curricular and extended school activities;
- ensure that pupils are fully aware of research skills and are made aware of legal issues relating to electronic content such as copyright laws.
- ensure that during lessons where internet use is pre-planned pupils are guided to sites checked as suitable for their use and that processes are known and used when dealing with any unsuitable material that is found in internet searches.

1.6 Pupils

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

- use the school ICT systems in accordance with instructions from staff;;

1.7 Parents

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

The key responsibilities for parents are to:

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

2. Training

2.1 Staff and Governor Training

This school:

- ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection;
- makes regular training available to staff on online safety issues and the school's online safety education programme as and when course/ sessions occur or are provided by the LA or our Health and Safety Consultants ;
- provides, as part of the induction process, all new staff (including those on university/college placements and work experience) and volunteers with information and guidance on the Online Safety Policy and procedures the school's Acceptable Use Agreements.

2.2 Parent Awareness

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

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

3. Teaching and Learning

3.1 Why Internet use is Important

- Internet use is part of the statutory curriculum and is a necessary tool for learning.
- The Internet is a part of everyday life for education, business and social interaction.
- The school has a duty to provide pupils with quality Internet access as part of their learning experience.
- Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.
- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management

functions.
- Internet access is an entitlement for pupils who show a responsible and mature approach to its use.

3.2 How Internet Use Benefits Education

Benefits of using the Internet in education include:

- access to worldwide educational resources including museums and art galleries;
- educational and cultural exchanges between pupils worldwide;
- vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across networks of schools, support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with the Local Authority and DfE;
- access to learning wherever and whenever convenient.

3.3 How Internet Use Enhances Learning

This school:

- plans Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas;
- ensures staff will model safe and responsible behaviour in their own use of technology during lessons;
- ensures that when copying materials from the web, staff understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights;
- ensures that staff understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include risks in pop-ups; buying online, online gaming/gambling etc.

3.4 Pupils with Additional Needs

Here are some considerations regarding possible ways to support a generic group of children who may require additional support to move forward in safeguarding themselves.

- *A fundamental part of teaching online safety is to check pupil's understanding and knowledge of general personal safety issues. Some pupils may need additional teaching that includes reminders and explicit prompts to link their existing knowledge of "how to keep safe" to the rules that will apply specifically to, for instance, internet use.*
- *This group of pupils are vulnerable to poor social understanding that may leave them open to risks when using the internet individually, but also when with peers.*
- *For various reasons, pupils with additional needs may find it difficult to explain or describe events when using the internet.*
- *Some pupils might find it easier to show adults what they did i.e. replay which will obviously have its own issues for staff regarding repeating access.*
- *Many of our pupils are very quick to click with the mouse and may not actually know what they did or how something happened. Gentle investigation will be more productive than asking many questions.*
- *Some pupils may not be able to ask for help. Staff will need to know specific pupils well so that this can be addressed.*
- *Pupils may need a system or a help sound set up on computers which will help them to get adult attention. If pupils don't recognise that they need help, then adult supervision is the safe way to improve their recognition of this.*

4. Managing Information Systems

4.1 Maintaining Information Systems Security

- **The security of the school information systems and users will be reviewed regularly.**
- **Virus protection will be updated regularly.**
- *Personal data sent over the Internet or taken off site will be encrypted.*
- *Portable media may not be used without specific permission followed by an anti-virus/malware scan.*
- *Unapproved software will not be allowed in work areas or attached to email.*
- *The ICT Support will review system capacity regularly.*
- *use of user logins and passwords to access the school network will be enforced – see Section 6.2 below.*

The school broadband and online suppliers are Online Systems and Cumbria Schools ICT Support.

4.2 Password Security

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

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

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

The management of password security will be the responsibility of the Clerical Assistant and ICT Support provider.

Responsibilities:

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

Passwords for new users and replacement passwords for existing users can be allocated by The Clerical Assistant. Any changes carried out must be notified to the member of staff responsible for issuing and coordinating password security (above).

Users will change their passwords every 90 days.

Training/Awareness:

It is essential that users are made aware of the need to keep passwords secure, and the risks attached to unauthorised access/data loss.

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

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

The following rules apply to the use of passwords:

- *passwords must be changed every* 90 days;
- *the last four passwords cannot be re-used;*
- *ideally the password should be a minimum of 8 characters long and must include three of – uppercase character, lowercase character, number, special character;*
- *the account should be "locked out" following six successive incorrect log-on attempts;*
- *temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on;*

- *passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption);*
- *requests for password changes should be authenticated by (the responsible person) to ensure that the new password can only be passed to the genuine user*

The "master/administrator" passwords for the school ICT system, used by the Clerical Assistant and ICT Support provider must also be available to the Headteacher or other nominated senior leader and kept in a secure place (e.g. school safe).

Audit/Monitoring/Reporting/Review:

The responsible person the Clerical Assistant will ensure that full records are kept of:

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

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

User lists, IDs and other security related information must be given the highest security classification and stored in a secure manner. These records will be reviewed by (Online Safety Coordinator/Online Safety Committee/Online Safety Governor) at regular intervals, as and when necessary or at the least when the Online Safety Policy is due for full review.

4.3 Managing Email

- **Staff will only use official school provided email accounts to communicate with parents, as approved by the Senior Leadership Team.**
- *Access in school to external personal email accounts may be blocked.*
- *Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be.*
- *The forwarding of chain messages is not permitted.*
- *Staff should not use personal email accounts during school hours or for professional purposes.*
- **The official school email service may be regarded as safe and secure and is monitored.** *Staff 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 need to be aware that email communications may be monitored.**
- **Users must immediately report, to the nominated person – in accordance with the school Policy and procedures, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.**
- **Any digital communication between staff and parents (email, chat, etc.) must be professional in tone and content.** *These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat/social networking programmes must not be used for these communications.*
- *Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.*
- *Spam, phishing and virus attachments can make email dangerous. The school ICT provider Cumbria Software Systems ensures mail is virus checked (ingoing and outgoing), includes spam filtering and backs emails up daily.*

4.4 Emailing Personal, Sensitive, Confidential or Classified Information

- Assess whether the information can be transmitted by other secure means before using email - emailing confidential data is not recommended and should be avoided where possible;
- The use of Hotmail, BTInternet, G-mail or any other Internet based webmail service for sending email containing sensitive information is not permitted;
- Where your conclusion is that email must be used to transmit such data:

- Obtain express consent from your manager to provide the information by email;
- Exercise caution when sending the email and always follow these checks before releasing the email:
    - Verify the details, including accurate email address, of any intended recipient of the information;
    - Verify (by phoning) the details of a requestor before responding to email requests for information;
    - Do not copy or forward the email to any more recipients than is absolutely necessary.
- Do not send the information to any person whose details you have been unable to separately verify (usually by phone);
- Send the information as an encrypted document **attached** to an email;
- Provide the encryption key or password by a **separate** contact with the recipient(s);
- Do not identify such information in the subject line of any email;
- Request confirmation of safe receipt.

4.5 Zombie Accounts

Zombie accounts refer to accounts belonging to users who have left the school and therefore no longer have authorised access to the school's systems. Such Zombie accounts when left active can cause a security threat by allowing unauthorised access.

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

Further advice is available at IT Governance Click here to access.

4.6 Managing Published Content

- **The contact details on the website are the school address, email and telephone number. Staff or pupils' personal information are not published.**
- *Email addresses will be published carefully online, to avoid being harvested for spam (e.g. by replacing '@' with 'AT'.)*
- *The headteacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.*
- *The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy procedures and copyright.*

4.7 Use of Digital and Video Images

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

- **We gain parental permission for the use of digital photographs or video involving their child as part of the school agreement form when their child joins the school. This is a once in a school lifetime consent. Parents are required to inform the school if their consent changes.**
- **We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs.**
-
- *Staff sign the school's Acceptable Use Agreement and this includes a clause on not using mobile phones/personal equipment for taking pictures of pupils;*
- *The school blocks/filter access to social networking sites or newsgroups*

- *Staff are allowed to take digital/video images to support educational aims, but must follow school procedures concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.*
- *Parents are prohibited from taking photographs in school or during school events such as Christmas concerts.*
- *Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.*
- *If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high profile publications the school will obtain individual parental permission for its long term use.*
- *Pupils' full names will not be used anywhere on the school website, particularly in association with photographs.*
- *Pupil's work can only be published with the permission of the parents.*

4.8 Managing Social Networking, Social Media and Personal Publishing Sites

- The school will control access to social media and social networking sites.
- Staff wishing to use educational internet materials 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.
- *All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.*
- *Concerns regarding a parents' use of social networking, social media and personal publishing sites (in or out of school) will be raised with the Headteacher.*
- *Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and outlined in the school Staff Acceptable Use Agreement – see Appendix F.*
- Further guidance can be found in the document 'Safe Use of Facebook and Other Social Networking Sites' on the KAHSC website.
- *A sample advice leaflet for parents on Social Networking Sites, in particular, Facebook, can be found at Appendix H.*

4.9 Managing Filtering

- *The school's broadband access will include filtering appropriate to the age and maturity of pupils.*
- *The school will work with the Schools Broadband team Online Systems and Cumbria Software Systems to ensure that filtering procedures are continually reviewed.*
- *The school will have a clear procedure for reporting breaches of filtering. All members of the school community (all staff and all pupils) will be aware of this procedure.*
- *If staff or pupils discover unsuitable sites, the URL will be reported to the Headteacher who will then record the incident and escalate the concern as appropriate.*
- *The School filtering system will block all sites on the Internet Watch Foundation (IWF) list Click here to access.*
- *Changes to the school filtering procedures will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Senior Leadership Team.*
- *The School Senior Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective.*
- *Any material that the school believes is illegal will be reported to appropriate agencies such as IWF Click here to access, Cumbria Police or CEOP* Click here to access.
- *The school's access strategy will be designed by educators to suit the age and curriculum requirements of the pupils, with advice from network managers.*

4.10 Webcams and CCTV

- *The school uses CCTV for security and safety. The only people with access to this are the staff and to access recorded footage, the Headteacher and Clerical Assistant only.*
- *Notification of CCTV use is displayed at the front of the school. Please refer to the Information Commissioners Office (ICO) for further guidance and the school CCTV procedures.*

- *We do not use webcams in school.*
- *Consent is sought from parents and staff on joining the school, in the same way as for all images.*

4.11 Managing Emerging Technologies

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

4.12 Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed;
- Processed for limited purposes;
- Adequate, relevant and not excessive;
- Accurate;
- Kept no longer than is necessary;
- Processed in accordance with the data subject's rights;
- Secure;
- Only transferred to others with adequate protection.

More detailed information can be found in the School Data Protection Policy.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

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

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

4.13 Disposal of Redundant ICT Equipment

- All redundant ICT equipment will be disposed of through an authorised agency. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
- All redundant ICT equipment that may have held personal data will have the storage media over written multiple times to ensure the data is irretrievably destroyed. Or if the storage media has failed it will be physically destroyed. We will only use authorised companies who will supply a written guarantee that this will happen.
- Disposal of any ICT equipment will conform to:
  - The Waste Electrical and Electronic Equipment Regulations 2006
  - The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007
  - Environment Agency Guidance (WEEE) Click here to access
  - ICO Guidance - Data Protection Act 1998 Click here to access
  - Electricity at Work Regulations 1989

- The school will maintain a comprehensive inventory of all its ICT equipment including a record of disposal.
- The school's disposal record will include:
  - Date item disposed of;
  - Authorisation for disposal, including:
    - verification of software licensing
    - any personal data likely to be held on the storage media? *
  - How it was disposed of e.g. waste, gift, sale
  - Name of person and/or organisation who received the disposed item

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

5. Policy Decisions

5.1 Authorising Internet Access

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

5.2 Assessing Risks

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor the LA can accept liability for the material accessed, or any consequences resulting from Internet use.
- The school will audit ICT use to establish if the Online Safety Policy and procedures is adequate and that the implementation of the Online Safety Policy is appropriate – see Appendix A for a sample Online Safety Audit.
- *The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Cumbria Police.*
- *Methods to identify, assess and minimise risks will be reviewed regularly.*

5.3 Unsuitable/Inappropriate Activities

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

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit	child sexual abuse images					✓

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation					✓
	adult material that potentially breaches the Obscene Publications Act in the UK					✓
	criminally racist material in UK					✓
	pornography				✓	
	promotion of any kind of discrimination				✓	
	promotion of racial or religious hatred				✓	
	threatening behaviour, including promotion of physical violence or mental harm				✓	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				✓	
Using school systems to run a private business					✓	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					✓	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					✓	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer / network access codes and passwords)					✓	
Creating or propagating computer viruses or other harmful files					✓	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet					✓	
Online gaming (educational)		✓				
Online gaming (non-educational)					✓	
Online gambling					✓	
Online shopping/commerce				✓		
File sharing				✓		
Use of social networking sites					✓	
Use of video broadcasting e.g. Youtube					✓	

5.4 What are the risks?

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

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

Byron Review (2008): Click here to access

5.5 Responding to Incidents of Concern

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

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- extremism or radicalisation of individuals
- other criminal conduct, activity or materials - school should refer to the Flow Chart found at Appendix I.
- *In this school there is strict monitoring and application of the Online Safety Policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions*
- *All members of the school community will be informed about the procedure for reporting online safety concerns (such as breaches of filtering, cyber-bullying, illegal content etc.).*
- *The Headteacher will record all reported incidents and actions taken in the School Online Safety incident log and other in any relevant areas e.g. Bullying or Child protection log.*
- *The Designated Safeguarding Lead will be informed of any online safety incidents involving Child Protection concerns, which will then be escalated appropriately – See Child Protection Policy and procedures for dealing with concerns.*
- *The school will manage Online Safety incidents in accordance with the school discipline/behaviour policy where appropriate.*
- *The school will inform parents of any incidents of concerns as and when required.*
- *After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.*
- *Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Safeguarding Hub* ***and*** *escalate the concern to the Police.*
- *If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Safeguarding Hub – see Child Protection Policy and procedures.*

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

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

Pupils **Actions / Sanctions**

Incidents:	Refer to class teacher/tutor	Refer to Head of Department/Head of Year/other	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering/security etc.	Inform parents	Removal of network / internet access rights	Warning	Further sanction e.g. detention/exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).			✓	✓		✓			
Unauthorised use of non-educational sites during lessons	✓					✓			
Unauthorised use of mobile phone / digital camera / other handheld device	✓					✓			
Unauthorised downloading or uploading of files	✓					✓			
Continued infringements of the above, following previous warnings or sanctions			✓			✓			
Accidentally accessing offensive or pornographic material and failing to report the incident	✓		✓			✓			
Deliberately accessing or trying to access offensive or pornographic material			✓			✓			

Staff **Actions / Sanctions**

Incidents:	Refer to line manager	Refer to Headteacher	Refer to LA/HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		✓	✓	✓			✓	✓
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email		✓				✓		
Unauthorised downloading or uploading of files		✓				✓		
Allowing others to access school network by sharing		✓	✓					✓

username and passwords or attempting to access or accessing the school network, using another person's account								
Careless use of personal data e.g. holding or transferring data in an insecure manner		✓						✓
Deliberate actions to breach data protection or network security rules		✓	✓				✓	✓
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		✓						✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		✓	✓				✓	✓
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils		✓	✓					✓
Actions which could compromise the staff member's professional standing		✓				✓		✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		✓				✓		✓
Using proxy sites or other means to subvert the school's filtering system		✓	✓			✓	✓	✓
Accidentally accessing offensive or pornographic material and failing to report the incident		✓	✓			✓		✓
Deliberately accessing or trying to access offensive or pornographic material		✓	✓	✓		✓	✓	✓
Breaching copyright or licensing regulations		✓				✓		
Continued infringements of the above, following previous warnings or sanctions		✓	✓			✓	✓	✓

5.6 Managing Cyber-bullying

- Cyber-bullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the Whole School Behaviour Policy.
- There are clear procedures in place to support anyone in the school community affected by cyber-bullying.
- All incidents of cyber-bullying reported to the school will be recorded.
- There will be clear procedures in place to investigate incidents or allegations of Cyber-bullying.
- *Pupils, staff and parents will be advised to keep a record of the bullying as evidence.*
- *The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.*
- *Pupils, staff and parents will be required to work with the school to support the approach to cyber-bullying and the school's online safety ethos.*
- *Sanctions for those involved in cyber-bullying may include:*
  - *The bully will be asked to remove any material deemed to be inappropriate or offensive.*
  - *A service provider may be contacted to remove content if the bully refuses or is unable to delete content.*
  - *Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance with the Whole School Behaviour Policy, Acceptable Use Agreement and Disciplinary Procedures.*
  - *Parents of pupils will be informed.*
  - *The Police will be contacted if a criminal offence is suspected.*

5.7 Managing Mobile Phones and Personal Devices

- The use of mobile phones and other personal devices by staff in school will be decided by the school and covered in the school Acceptable Use Agreement.

- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school discipline/Behaviour Policy.
- The school reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable materials, including those which promote pornography, violence or bullying. Staff mobiles or hand-held devices may be searched at any time as part of routine monitoring.
- School staff may confiscate a phone or device if they believe it is being used to contravene the school's behaviour Policy or bullying procedures.
- *If there is suspicion that the material on the mobile may provide evidence relating to a criminal offence the phone will be handed over to the police for further investigation.*
- *Mobile phones and personal devices will not be used during lessons or formal school time unless as part of an approved and directed curriculum based activity with consent from a member of staff. They should be placed on silent and stored out of sight in the staffroom at school. Staff members may use their phones during school break times. All visitors are requested to keep their phones on silent and in the staffroom or office whilst in the school.*
- *The recording, taking and sharing of images, video and audio on any mobile phone is not allowed.*
- *The Bluetooth function of a mobile phone should be switched off at all times.*
- *Electronic devices of all kinds that are brought in to school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.*
- *Staff may use their phones 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 times other than their break time. The school office number can be given as an alternative contact number for staff members.*
- *Mobile phones and personal devices are not permitted to be used other than in the staff room.*

Parents' use of personal devices:

- *Parent's mobile phones are not to be used in school.*

Staff use of personal devices:

- *Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.*
- *Staff will be issued with a school phone where contact with pupils or parents is required.*
- *Mobile phones and personally owned devices will be switched off or switched to 'silent' mode; Bluetooth communication should be "hidden" or switched off and mobile phones or personally owned devices will not be used during teaching periods unless permission has been given by a member of Senior Leadership Team in emergency circumstances.*
- *Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose.*
- *Where members of staff are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, , then the school office will be contacted to make the call to parents. 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.*
- *If a member of staff breaches the school Policy and procedures then disciplinary action may be taken.*

	Staff & other adults				**Pupils**			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed

Mobile phones may be brought to school	✓							✓
Use of mobile phones in lessons				✓				✓
Use of mobile phones in social time	✓							✓
Taking photos on mobile phones or other camera devices				✓				✓
Use of hand held devices e.g. PDAs, PSPs		✓						✓
Use of personal email addresses in school, or on school network				✓				✓
Use of school email for personal emails				✓				✓
Use of chat rooms/facilities				✓				✓
Use of instant messaging				✓				✓
Use of social networking sites				✓				✓
Use of blogs				✓				✓

6. Communicating Policy and procedures

6.1 Introducing the Policy and procedures to Pupils

Due to the age of our young children the teaching of online safety forms part of our Personal Safety Awareness Curriculum.

Useful online safety programmes include:

- Think U Know: www.thinkuknow.co.uk
- Childnet: www.childnet.com
- Kidsmart: www.kidsmart.org.uk
- All users will be informed that Internet use will be monitored.
- *Pupil instruction regarding responsible and safe use will precede Internet access.*
- *An online safety module will be included in the age appropriate curriculum covering both safe school and home use.*
- *Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.*
- *Particular attention to Online Safety education will be given where pupils are considered to be vulnerable.*

6.2 Discussing the Policy and procedures with Staff

- The Online Safety Policy and procedures will be formally provided to, and discussed, with all members of staff.
- To protect all staff and pupils, the school will implement Acceptable Use Agreements.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.
- *Staff who manage filtering systems or monitor ICT use will be supervised by the Senior Leadership Team and have clear procedures for reporting issues.*
- *The School will highlight useful online tools which staff should use with children in the classroom. These tools will vary according to the age and ability of the pupils.*

- *All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.*

6.3 Enlisting Parents' Support

- Parents' attention will be drawn to the school Online Safety Policy when their child joins the school
- *A partnership approach to online safety at home and at school with parents will be encouraged.*
- *Parents will be requested to agree to an Online Safety/Internet agreement.*
- *Information and guidance for parents on online safety will be made available to parents in a variety of formats.*
- *Advice on useful resources and websites, filtering systems and educational and leisure activities which include responsible use of the Internet will be made available to parents.*
- *Interested parents will be referred to organisations listed in the "online safety Links" at Appendix K.*

7. Complaints

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

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

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

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

Any complaint about staff misuse is referred to the Head teacher.

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

8. Acknowledgements

With thanks to Jeff Haslam (E-Safety Consultant), Hertfordshire County Council, Kent County Council, the South West Grid for Learning, Cumbria LSCB, CEOP, UKCCIS, Childnet and the DfE whose guidance and information has contributed to the development of this Policy and procedures.

CLEATOR MOOR NURSERY SCHOOL ONLINE SAFETY AUDIT

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

Does the school have an Online Safety Policy and procedures	**YES ~~/ NO~~**
Date of latest update:	January 2018
Date of future review:	January 2021 (with annual monitoring)
The school Online Safety Policy and procedures was agreed by governors on:	
The Policy and procedures is available for staff to access at:	The Policy Library in the meeting room
The Policy and procedures is available for parents to access at:	Via request to the Headteacher
The responsible member of the Senior Leadership Team is:	Beverley Prescott
The Governor responsible for Online Safety is:	Lisa Wilson
The Designated Safeguarding Lead is:	Lisa Wilson
The Online Safety Coordinator is:	N/A
Were all stakeholders (e.g. pupils, staff and parents) consulted when updating the school Online Safety Policy and procedures?	**~~YES /~~ NO**
Has up-to-date Online Safety training been provided for all members of staff? (not just teaching staff)	**YES ~~/ NO~~**
Do all members of staff sign an Acceptable Use Agreement on appointment?	**YES ~~/ NO~~**
Are all staff made aware of the schools expectation around safe and professional online behaviour?	**YES ~~/ NO~~**
Is there a clear procedure for staff, pupils and parents to follow when responding to or reporting an online safety incident of concern?	**YES ~~/ NO~~**
Have online safety materials from CEOP, Childnet and UKCCIS etc. been obtained?	**YES ~~/ NO~~**
Is online safety training provided for all pupils (appropriate to age and ability)?	**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?	**~~N/A~~**
Do parents sign an Acceptable Use Agreement?	**~~YES /~~ NO**
Are staff, parents and visitors aware that Internet use is closely monitored and individual usage can be traced?	**YES ~~/ NO~~**
Has an ICT security audit been initiated by Headteacher?	**YES ~~/ NO~~**
Is personal data collected, stored and used according to the principles of the Data Protection Act?	**YES ~~/ NO~~**
Is Internet access provided by an approved educational Internet service provider which complies with DfE requirements?	**YES ~~/ NO~~**
Has the school filtering been designed to reflect educational objectives and been approved by Headteacher?	**YES ~~/ NO~~**
Are members of staff with responsibility for managing filtering, network access and monitoring systems adequately supervised by a member of Headteacher?	**N/A**
Does the school log and record all online safety incidents, including any action taken?	**YES ~~/ NO~~**
Are the Governing Body and Headteacher monitoring and evaluating the school Online Safety Policy and procedures on a regular basis?	**YES ~~/ NO~~**

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.

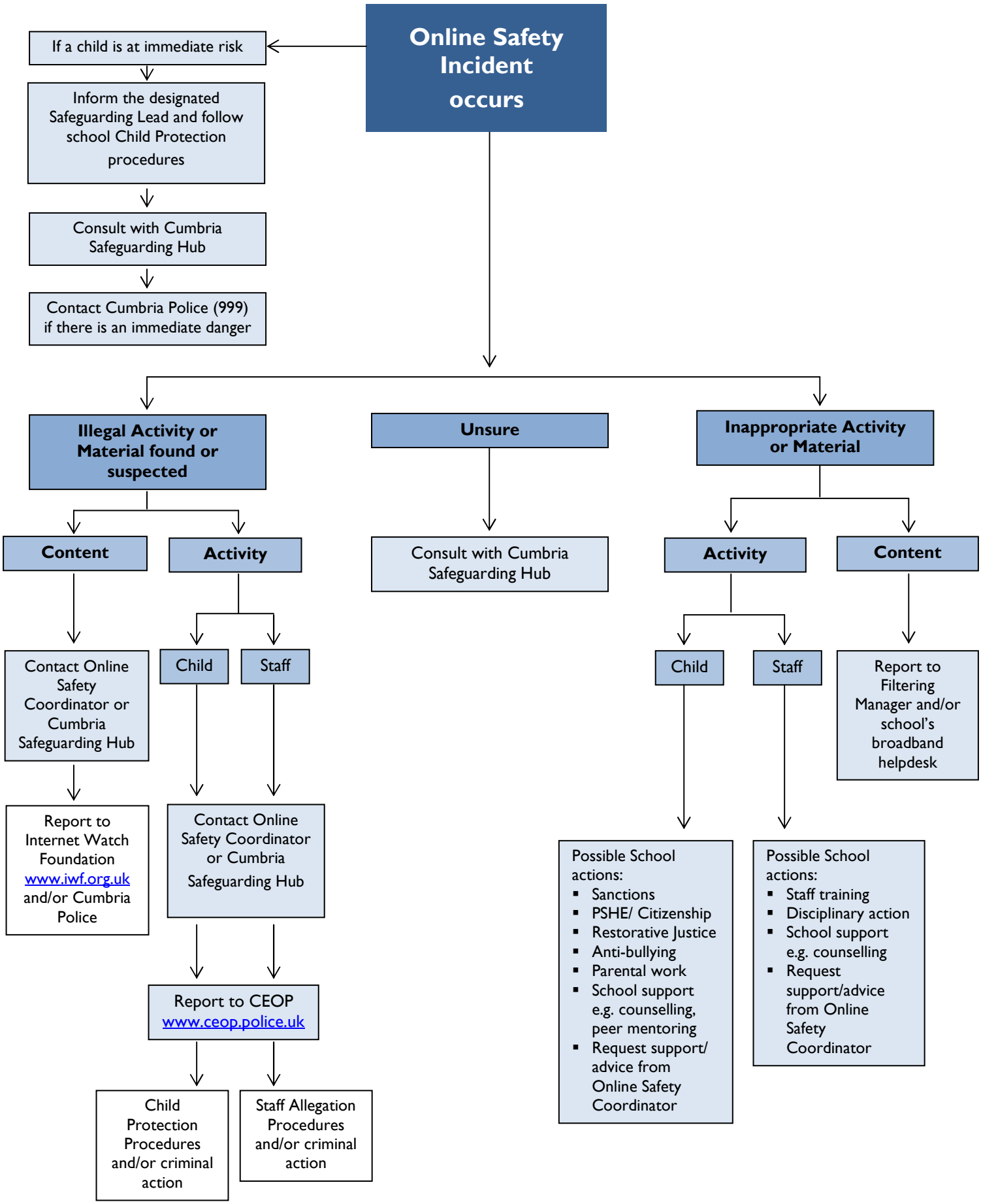
Should you decide to allow your children to have a Facebook profile we strongly advise you to:

- 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 school Online Safety Policy and procedures; record actions in Online Safety incident log and implement any changes in the future.

CLEATOR MOOR NURSERY SCHOOL - ONLINE SAFETY INCIDENT LOG

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

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

ONLINE SAFETY LINKS

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

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

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

Department for Education/Home Office guidance for schools

PREVENT Duty statutory guidance for Public Bodies: England and Wales – March 2015
The PREVENT Duty – non-statutory Departmental advice for Schools and Childcare Providers – DfE – June 2015
How Social Media is used to encourage travel to Syria and Iraq – Home Office advice to schools – June 2015

LEGAL FRAMEWORK

Protection of Children Act 1978
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Racial and Religious Hatred Act 2006
This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

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

Sexual Offences Act 2003
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). This can include images taken by and distributed by the child themselves (often referred to as "Sexting"). A person convicted of such an offence may face up to 10 years in prison.

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

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

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

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

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

Communications Act 2003 (section 127)
Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Data Protection Act 1998
This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Not kept longer than necessary
- Processed in accordance with the data subject's rights
- Secure

- Not transferred to other countries without adequate protection

The Computer Misuse Act 1990 (sections 1 - 3)
This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

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

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

Copyright, Design and Patents Act 1988
Copyright is the right to prevent others from copying or using his or her "work" without permission. The material to which copyright may attach (known in the business as "work") must be the author's own creation and the result of some skill and judgement. It comes about when an individual expresses an idea in a tangible form. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer.

It is an infringement of copyright to copy all or a substantial part of anyone's work without obtaining the author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

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

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

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

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

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

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

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;

- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Criminal Justice and Immigration Act 2008
Section 63 offence to possess "extreme pornographic image"
63 (6) must be "grossly offensive, disgusting or otherwise obscene"
63 (7) this includes images of "threats to a person life or injury to anus, breasts or genitals, sexual acts with a corpse or animal whether alive or dead" must also be "explicit and realistic". Penalties can be up to 3 years imprisonment.

Education and Inspections Act 2006
Education and Inspections Act 2006 outlines legal powers for schools which relate to Cyber-bullying/ Bullying:

- Head teachers have the power "to such an extent as is reasonable" to regulate the conduct of pupils off site.
- School staff are able to confiscate items such as mobile phones etc. when they are being used to cause a disturbance in class or otherwise contravene the school behaviour/anti-bullying procedures.

Telecommunications Act 1984
It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994
This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Human Rights Act 1998
This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial.
- The right to respect for private and family life, home and correspondence.
- Freedom of thought, conscience and religion.
- Freedom of expression.
- Freedom of assembly.
- Prohibition of discrimination.
- The right to education.

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

GLOSSARY OF TERMS

Becta	British Educational Communications and Technology Agency (Government agency promoting the use of information and communications technology) – *NOTE: Becta Closed in 2011*
CEOP	Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CLEO	The Regional Broadband Consortium of Cumbria and Lancashire – is the provider of broadband and other services for schools and other organisations in Cumbria and Lancashire
CPD	Continuous Professional Development
DfE	Department for Education
FOSI	Family Online Safety Institute
HSTF	Home Secretary's Task Force on Child Protection on the Internet
ICO	Information Commissioners Office
ICT	Information and Communications Technology
ICTMark	Quality standard for schools provided by Naace Click here to access
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
JANET	Provides the broadband backbone structure for Higher Education and for the National Education Network.
KS1	Key Stage 1 (2, 3, 4 or 5) – schools are structured within these multiple age groups e.g. KS3 = years 7 to 9 (age 11 to 14)
LA	Local Authority
LAN	Local Area Network
Learning Platform	A learning platform brings together hardware, software and supporting services to support teaching, learning, management and administration.
LSCB	Local Safeguarding Children Board
MIS	Management Information System
MLE	Managed Learning Environment
NEN	National Education Network – works with the Regional Broadband Consortia (e.g. CLEO in Cumbria) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
Ofsted	Office for Standards in Education, Children's Services and Skills
PDA	Personal Digital Assistant (handheld device)
PHSE	Personal, Health and Social Education
RBC	Regional Broadband Consortia (e.g. CLEO) have been established to procure broadband connectivity for schools in England. There are 13 RBCs covering most local authorities in England, Wales and Northern Ireland.
SEF	Self Evaluation Form – used by schools for self-evaluation and reviewed by Ofsted prior to visiting schools for an inspection
TUK	Think U Know – educational E-Safety programmes for schools, young people and parents.
URL	Uniform Resource Locator (URL) it is the global address of documents and other resources on the World Wide Web.
VLE	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,
WAP	Wireless Application Protocol