Cauldwell School

SH019	**Version 1**	**Online Safety Policy**	
Co-ordinator:	Sarah Degning		
Link Governor:			
Approval:			
Document Location:	• Curriculum Policy Folder on VLE • School website.		
Review Frequency:		**Review Date:**	

Document History:

Version	Description	Date	By
1.0	Reviewed by co-ordinator, no amendment. No link governor at the moment.	26/02/2017	SD
1.0	Filed in folder and on VLE. Copy on website.	01/03/2017	

1. VISION

At Cauldwell, we are committed to providing our children with the skills, knowledge and understanding of computing that will help them meet the challenges and opportunities of the 21st century. In computing, children will learn the fundamental principles of computing in a practical and creative way so they can develop problem solving and logic skills, understand how computers and computer systems work, design and build programs, develop their ideas using technology and create a range of content.

2. VALUES

Cauldwell School
Committed To Achievement for All

3. PURPOSE

The purpose of this policy, which incorporates the Acceptable Use Policy, is to:

- Set out the key principles expected of all members of the school community at Cauldwell School with respect to the use of IT-based technologies.
- Safeguard and protect the children and staff of Cauldwell School.
- Assist school staff working with children to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use.
- Have clear structures to deal with online abuse such as online bullying which are cross referenced with other school policies.
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with pupils.
- It applies to all members of the Cauldwell School community, including, staff, pupils, volunteers, parents/carers, visitors and community users who have access to and are users of school Computing systems, both in and out of Cauldwell School; it ensures that pupils, staff and all others in the school community are able to use the internet and related communications technologies appropriately and safely and is part of the wider duty of care to which all who work in schools are bound.

- This framework of online safety, or acceptable user policy (AUP), is to promote safe and appropriate use. As such, it should be understood in the context of other 'child protection' and 'behaviour' policies that the school already has in place as well as other existing policies in respect of its employees.

  The main areas of risk for our school community can be summarised as follows:

  Content
  Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse
  - Hate sites
  - Content validation: how to check authenticity and accuracy of online content

  Contact
  - Grooming
  - Online bullying in all forms
  - Identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords

  Conduct
  - Privacy issues, including disclosure of personal information
  - Digital footprint and online reputation
  - Health and well-being (amount of time spent online (Internet or gaming)) Sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)
  - Extremism (see Prevent policy)
  - Copyright (little care or consideration for intellectual property and ownership – such as music and film)

  (Ref Ofsted 2013)

  Communication:
  The policy will be communicated to staff/pupils/community in the following ways:
  - Policy to be posted on the school website
  - Policy to be part of school induction pack for new staff
  - Acceptable use agreements discussed with pupils at the start of each year.
  - Acceptable use agreements to be issued to whole school community, usually on entry to the school
  - Acceptable use agreements to be held in pupil and personnel files

  Handling 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 material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

- Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available may include: ○ Interview by teacher / Team leader/ Headteacher; ○ Informing parents or carers; ○ Removal of Internet or computer access for a period ○ Referral to LA / Police.

- The school's Online Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.

- Complaints of online bullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with the school's child protection procedures.

4. POLICY

This policy, covers the following areas:

Education and Curriculum

Pupil Online safety curriculum

In order to match electronic resources as closely as possible to the national and school curriculum, teachers need to review and evaluate resources in order to offer materials that are appropriate to the age range and ability of the group being taught. The class teacher will provide appropriate guidance to pupils as they make use of the internet to conduct research and other studies. All pupils will be informed by staff of their rights and responsibilities as users, before their first use, either as an individual user or as a member of a class or group.

While pupils may be able to move beyond those resources which have been evaluated by staff, they shall be provided with guidelines and lists of resources particularly suited to the learning objectives. Pupils may not pursue electronic research independent of staff supervision. The schools internet access is controlled by filtering software chosen by Bedford Borough Council, which should stop access to many inappropriate sites, although we recognise that no system is totally secure. Staff should ensure children use the search browser *Yahoo*. Only staff should use *Google*.

The staff are aware that all inappropriate sites accidentally accessed in school should be reported to the ICT Co-ordinator, Head teacher and then to Bedford I.Tec.

- **-NB- Bedford Borough filters sites but photos are filtered by *text description* and NOT content (thus, inappropriate images can be displayed).**

This school:

- Has a clear, progressive Online safety education programme as part of the Computing curriculum / PSHE curriculum.

The school has developed a set of guidelines for Internet use by pupils. These rules will be made available to all pupils and kept under constant review. All members of staff are responsible for explaining the rules and their implication. All members of staff need to be aware of possible misuses of on-line access and their responsibilities towards pupils. This covers a range of skills and behaviours appropriate to their age and experience, including:

- To STOP and THINK before they CLICK
- To develop a range of strategies to evaluate and verify information before accepting its accuracy;
- To be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
- To know how to narrow down or refine a search; ○ To understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
- To understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
- To understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned on privacy settings;
- To understand why they must not post pictures or videos of others without their permission;
- To know not to download any files – such as music files - without permission;
- To have strategies for dealing with receipt of inappropriate materials; ○ To understand the impact of online bullying, sexting, extremism and trolling and know how to seek help if they are affected by any form of online bullying.
- To know how to report any abuse including online bullying; and how to seek help if they experience problems when using the Internet and related technologies, i.e. parent or carer, teacher or trusted staff

member, or an organisation such as ChildLine or the CLICK CEOP button.

- It plans Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.

- Will remind pupils about their responsibilities; Pupils are taught that access is a privilege, not a right and that access requires responsibility. It is presumed that users will comply with school standards and will honour the values the school holds. The school may review files and communications to ensure that users are using the system responsibly. Users should not expect that files stored on servers or disks will always be private.

- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons.

- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights;

- Ensures that during school, teachers will guide pupils toward appropriate materials. Outside of school, families bear responsibility for such guidance, as they must also exercise with information sources such as television, telephones, films, radio and other potential offensive media.

The following will not be tolerated:

- Sending or displaying offensive messages or pictures
- Using obscene language
- Harassing or insulting others
- Damaging computers, computer systems or computer networks
- Violating copyright laws by downloading copyrighted items
- Using others' passwords
- Trespassing in others' folders, work or files

Sanctions: Violations of the above rules will result in a temporary or permanent ban on internet use in school. Teachers should ensure that any violation of internet use, as defined above, should be recorded in the child's Well-being Record; Additional disciplinary action may be added in line with existing practice on inappropriate language or behaviour.

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 program;
- Provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the Online Safety /the school's Acceptable Use Policy.

Parent awareness and training

This school:

- Provides advice, guidance and training for parents, including:
    - Introduction of the Acceptable Use Agreements to new parents, to ensure that principles of online safe behaviour are made clear
    - Information leaflets; in school newsletters; on the school web site;
    - Demonstrations, practical sessions held at school;
    - Suggestions for safe Internet use at home;
    - Provision of information about national support sites for parents.

Expected Conduct and Incident management

In this school, all users:

- Are responsible for using the school Computing systems in accordance with the relevant Acceptable Use Policy which they will be expected to sign before being given access to school systems. Need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Should 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 covers their actions out of school, if related to their membership of the school
- Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on online bullying

Staff:

- Are responsible for reading the school's Online safety policy and using the school Computing systems accordingly, including the use of mobile phones, and hand held devices.

Pupils:

- Should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

Parents/Carers:

- Should provide consent for pupils to use the Internet, as well as other technologies, as part of the Online safety acceptable use agreement form at time of their child's entry to the school
- should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse

Incident Management

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 and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes.

- Support is actively sought from other agencies as needed in dealing with online safety issues
- Monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in e-safety within the school. The records are reviewed/audited and reported to the school's senior leaders, Governors /the LA / LSCB

  Parents / carers are specifically informed of online safety incidents involving young people for whom they are responsible.

- We will contact the Police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law

Managing the IT and Computing infrastructure, covering: Internet access, security (virus protection) and filtering

This school:

- Has the educational filtered secure broadband connectivity through the LA ○ Uses the LA filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc.
- Has blocked pupil access to music download or shopping sites – except those approved for educational purposes at a regional or national level;
- Uses security time-outs on Internet access where practicable / useful; ○ Works in partnership with the LA and Technical service provider to ensure any concerns about the system are communicated so that systems remain robust and protect pupils;
- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable;
- Ensures all staff and pupils have signed an acceptable use agreement form and understands that they must report any concerns;
- Ensures pupils only publish within an appropriately secure environment:
- the school's learning environment/ Learning Platform.
- Requires staff to preview websites before use [where not previously viewed or cached] and encourages use of the school's Learning Platform as a key way to direct pupils to age / subject appropriate web sites; Plans the curriculum context for Internet use to match pupils' ability, using childfriendly search engines where more open Internet searching is required; e.g. yahoo for kids or ask for kids , Google Safe Search. ○ Never allows / Is vigilant when conducting 'raw' image search with pupils
- e.g. Google image search;
- Informs all users that Internet use is monitored;
- Informs staff and pupils that that they must report any failure of the filtering systems directly to the *teacher / responsible adult / Computing*
- *Coordinator. The Computer cCoordinator will log/* escalates as appropriate to the Technical service provider or the LA Helpdesk as necessary; ○ Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme;
- Provides advice and information on reporting offensive materials, abuse/ bullying etc. available for pupils, staff and parents
- Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA.

Network management (user access, backup)

This school

- Uses individual, audited log-ins for all users on the school's Learning Platform;
- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services

- Ensures the Computer Coordinator is up-to-date with LA services and policies / requires the Technical Support Provider to be up-to-date with LA services and policies;
- Storage of all data within the school will conform to the UK data protection requirements;
- Pupils and Staff using mobile technology, where storage of data is online, will conform to the EU data protection directive where storage is hosted within the EU.

To ensure the network is used safely, this school:

- Ensures staff read and sign that they have understood the school's Online safety Policy.
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network;
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
- Requires all users to always log off when they have finished working or are leaving the computer unattended;
- Requests that teachers and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed. We request that they DO switch the computers off at the end of the day and we also automatically switch off all computers at 18:00 hours to save energy;
- Has set-up the network so that users cannot download executable files / programmes;
- Has blocked access to music/media download or shopping sites – except those approved for educational purposes;
- Scans all mobile equipment with anti-virus / spyware before it is connected to the network;
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so;
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs.

- Maintains equipment to ensure Health and Safety is followed, e.g. projector filters cleaned by our Technical service provider; equipment installed and checked by approved Suppliers / LA electrical engineers;
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems;
  e.g. technical support or MIS Support;
- Provides pupils and staff with access to content and resources through the approved Learning Platform which staff and pupils access using their username and password;
- Makes clear responsibilities for the daily back up of MIS and finance systems and other important files;
- Has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data, that complies with external Audit's requirements;
- Uses the DfE secure s2s website for all CTF files sent to other schools;
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA;
- Follows ISP advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use;
- All computer equipment is installed professionally and meets health and safety standards;
- Projectors are maintained so that the quality of presentation remains high;
- Reviews the school IT systems regularly with regard to health and safety and security.

Passwords

- This school makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find it;
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private.
- It is accepted that from time to time, e.g. forgetting a password, the Computer (Vle) co-ordinator can help to create a new password but s/he will not know what it is.

- Computers must not be left in 'logged on' mode. It is good practice for users to change their passwords regularly. Laptops are to be password protected at all times.

Email This school

- Provides staff with an email account for their professional use, *name@cauldwell.org.uk* and makes clear personal email should be through a separate account;
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date
- Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police.

Pupils:

- Pupils are introduced to, and use e-mail (*messages* only facility on the school's Learning Platform) as part of the Computing scheme of work.
- Pupils are taught about the online safety and 'netiquette' of using e-mail both in school and at home i.e. they are taught:
    - Not to give out their e-mail address unless it is part of a school managed project or to someone they know and trust and is approved by their teacher or parent/carer;
    - That an e-mail is a form of publishing where the message should be clear, short and concise;
    - That any e-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper;
    - They must not reveal private details of themselves or others in e-mail, such as address, telephone number, etc.;
    - To 'Stop and Think Before They Click' and not open attachments unless sure the source is safe;
    - That they should think carefully before sending any attachments; ○ embedding adverts is not allowed;
    - That they must immediately tell a teacher / responsible adult if they receive an e-mail which makes them feel uncomfortable, is offensive or bullying in nature;
    - Not to respond to malicious or threatening messages; ○ Not to delete malicious of threatening e-mails, but to keep them as evidence of bullying;

- Not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them;
- That forwarding 'chain' e-mail letters is not permitted.

Staff:

- Staff can only use the e mail systems on the school's Learning platform for professional purposes
- Staff know that e-mail sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on school headed paper. That it should follow the school 'house-style':
  - the sending of multiple or large attachments should be limited, and may also be restricted by the provider of the service being used;
  - the sending of chain letters is not permitted;
  - embedding adverts is not allowed;
- All staff sign our school Agreement Form AUP to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

School website

- The Headteacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- Uploading of information is restricted to our website authorisers, Office Manager
- The school web site complies with the statutory DfE guidelines for publications;
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- The point of contact on the web site is the school address, telephone number and we use a general email contact address, e.g. schooloffice@cauldwell.org.uk. Home information or individual e-mail identities will not be published;
- Photographs published on the web do not have full names attached;
- We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website;
- We do not use embedded geodata in respect of stored images We expect teachers using school approved blogs or wikis to password protect them and run from the school website.

Learning platform

- Uploading of information on the schools' Learning Platform / virtual learning space is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas;
- Photographs and videos uploaded to the schools LEARNING PLATFORM will only be accessible by members of the school community;
- In school, pupils are only able to upload and publish within school approved and closed systems, such as the Learning Platform;

Social networking

School staff will ensure that in private use:

- No reference should be made in social media to pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Data security: Management Information System access and Data transfer

Strategic and operational practices

At this school:

- The Head Teacher is the Senior Information Risk Officer (SIRO).
- Staff are clear who are the key contact(s) for key school information (the Information Asset Owners) are.
- We ensure staff know who to report any incidents where data protection may have been compromised.
- All staff are DBS checked and records are held in one central record;
- We ensure ALL the following school stakeholders sign an Acceptable Use Agreement form. We have a system so we know who has signed.

  ○ staff, ○ governors, ○ pupils ○ parents

  This makes clear staffs' responsibilities with regard to data security, passwords and access.

- We follow LA guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services.
- We require that any Protect and Restricted material must be encrypted if the material is to be removed from the school and limit such data removal.
- School staff with access to setting-up usernames and passwords for email, network access and Learning Platform access are working within the approved system and follow the security processes required by those systems.
- We ask staff to undertaken at least annual house-keeping to review, remove and destroy any digital materials and documents which need no longer be stored.

- **Sanctions:**
  Pupils who deliberately abuse the AUP will be dealt with in line with the school's Behaviour Policy. Parents must be informed and any incident must be logged in school by the SIRO.

Technical Solutions

- Staff have secure area(s) on the network to store sensitive documents or photographs.
- We require staff to log-out of the *staff* systems when leaving their computer, but also enforce lock-out after 10 minutes idle time.
- We use <encrypted flash drives> if any member of staff has to take any sensitive information off site.
- We store any Protect and Restricted written material in lockable storage cabinets in a lockable storage area.
- All servers are in lockable locations and managed by DBS-checked staff.
- We lock any back-up tapes in a secure, fire-proof cabinet.
- We comply with the WEEE directive on equipment disposal by using an approved or recommended disposal company for disposal of equipment where any protected or restricted data has been held and get a certificate of secure deletion for any server that once contained personal data.
- Paper based sensitive information is shredded, using cross cut shredder / collected by secure data disposal service.

Equipment and Digital Content

Personal mobile phones and mobile devices

- Mobile phones brought into school are entirely at the staff member, pupils & parents' or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school. Pupil's mobile phones that are brought into school must be turned off (not placed on silent) and handed in to the school office upon arrival at school. Staff members may use their phones during school break times. All visitors are requested to keep their phones on silent.

- The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided; except where it has been explicitly agreed otherwise by the Headteacher. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Headteacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.

- 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 material, 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.

- Where parents or pupils need to contact each other during the school day, they should do so only through the School's telephone. Staff may use their phones during break times. If 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 times.

- Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.

- Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.

- Mobile phones and personally-owned devices are not permitted to be used in certain areas within the school site, e.g. changing rooms and toilets.

- Mobile phones 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.

- The Bluetooth or similar 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.

- No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned.

Students' use of personal devices

- The School strongly advises that pupil's mobile phones should not be brought into school.
- 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. Pupils will hand their phone into the school office at the start of the day and collect it at the end of day from the UKS2 team leader/head teacher.

Staff use of personal devices

- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.
- Staff will be issued with a school phone where contact with students, parents or carers 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 granted by a member of the senior leadership team in emergency circumstances.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting students or parents, then a school mobile phone will be provided and used. In an emergency where a staff member doesn't 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.

Digital images and video

In this school:

- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school;
- 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 Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils;

- If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long term use
- The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose;
- Pupils are taught about how images can be manipulated in their e-safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their IT scheme of work;
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identify of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Asset disposal

- Details of all school-owned hardware will be recorded in a hardware inventory.
- Details of all school-owned software will be recorded in a software inventory.
- All redundant equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
- All redundant equipment that may have held personal data will have the storage media forensically wiped. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen
- Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.

5. MONITORING, EVALUATION AND REVIEW

- The Online safety policy is referenced from within other school policies: Computing policy, Child Protection policy, Anti-Bullying policy and in the School Development Plan, Behaviour policy, Personal, Social and Health Education, Citizenship and Mobile Phone policies.

- The Computing Co-ordinator is responsible for document ownership, review and updates.

- The Online safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school.

- The Online safety policy has been written by the school Online safety Coordinator and is current and appropriate for its intended audience and purpose.

- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors. All amendments to the school online safeguarding policy will be discussed in detail with all members of teaching staff.
- This policy will be reviewed within one year of its first ratification by the school Governors.

Appendix

Role	Key Responsibilities
Headteacher Computing / online safety co-ordinator / Designated Child Protection Lead	To take overall responsibility for Online Safety provision To take overall responsibility for data and data security (SIRO) To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements To be responsible for ensuring that staff receive suitable training to carry out their Online safety roles and to train other colleagues, as relevant To be aware of procedures to be followed in the event of a serious esafety incident. Takes day to day responsibility for Online safety issues and has a leading role in establishing and reviewing the school Online safety policies / documents Promotes an awareness and commitment to Online safeguarding throughout the school community Ensures that Online safety education is embedded across the curriculum To communicate regularly with SLT and the designated Online safety Governor / committee to discuss current issues, review incident logs and filtering / change control logs To ensure that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident To ensure that an Online safety incident log is kept up to date Facilitates training and advice for all staff Liaises with the Local Authority and relevant agencies Is regularly updated in e-safety issues and legislation, and be aware of the potential for serious child protection issues to arise from: • sharing of personal data • access to illegal / inappropriate materials • inappropriate on-line contact with adults / strangers • potential or actual incidents of grooming • Online bullying and use of social media
Governors / Online safety governor	To ensure that the school follows all current Online safety advice to keep the children and staff safe To approve the Online Safety Policy and review the effectiveness of the policy. This will be carried out by the Governors / Governors Sub Committee receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor To support the school in encouraging parents and the wider community to become engaged in e-safety activities The role of the Online Safety Governor will include: • regular review with the Online Safety Co-ordinator / Officer (including Online safety incident logs, filtering / change control logs)

Role	Key Responsibilities
Computing Co-ordinator	To oversee the delivery of the online safety element of the Computing curriculum To liaise with the online safety coordinator regularly
Technical support (Partnership)	To report any online safety related issues that arise, to the Online safety coordinator. To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed To ensure that provision exists for misuse detection and malicious attack e.g. Keeping virus protection up to date) To ensure the security of the school IT system • the school's policy on web filtering is applied and updated on a regular basis • Bedford Borough is informed of issues relating to the filtering applied by the LA • that he / she keeps up to date with the school's Online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.
LEARNING PLATFORM (Computing Coordinator)	To ensure that all data held on pupils on the LEARNING PLATFORM is adequately protected
School Office Manager	To ensure that all data held on pupils on the school office machines have appropriate access controls in place
Teachers	To embed online safety issues in all aspects of the curriculum and other school activities To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant) To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
All staff	To read, understand and help promote the school's e-safety policies and guidance To read, understand, sign and adhere to the school staff Acceptable Use Agreement / Online Safety Policy To 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 policies with regard to these devices To report any suspected misuse or problem to the online safety coordinator To maintain an awareness of current online safety issues and guidance e.g. Through CPD To model safe, responsible and professional behaviours in their own use of technology

	To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. Email, text, mobile phones etc.
Role	Key Responsibilities
Pupils	Read, understand, sign and adhere to the Pupil Acceptable Use Policy (included as part of the Home/School agreement) Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations To understand the importance of reporting abuse, misuse or access to inappropriate materials To know what action to take if they or someone they know feels worried or vulnerable when using online technology. To know and understand school policy on the use of mobile phones, digital cameras and hand held devices. To know and understand school policy on the taking / use of images and on cyber-bullying. To 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 covers their actions out of school, if related to their membership of the school To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home.
Parent Liaison Officer	Educating Parents and raising awareness of how to stay/remain safe online at home.
Parents/carers	To support the school in promoting online safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images To read, understand and promote the school Pupil Acceptable Use Agreement with their children To access the school website / LEARNING PLATFORM / on-line student / pupil records in accordance with the relevant school Acceptable Use Agreement. To consult with the school if they have any concerns about their children's use of technology

External groups	Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the Internet within school (see Appendix)

Pupils' internet Safety Rules

RULES FOR ONLINE SAFETY AT CAULDWELL SCHOOL

1. I will always ask the teacher before I use the Internet and will be sensible whenever I use it.

2. I will only use the Internet for schoolwork and will only use the sites my teacher has asked me to access.

3. I will not give my name, address or telephone number to anyone on the Internet and I will tell the teacher if anyone asks me for my name, address or telephone number.

4. I will never agree to meet someone I have spoken to on the Internet.

5. I will not download programmes or bring programmes on disc, CD Rom or memory sticks from home into school.

6. I will only e-mail the people my teacher has approved and the message I send will be polite and responsible.

7. I will report any unpleasant material or messages sent to me. I understand this report would be confidential and would help protect other pupils and myself.

8. I realise that if I don't use the Internet sensibly I will not be allowed to use it.

Pupil Name: _____ Signature: _____

I have read and understand the above.

The SIRO will maintain an incident log and report on its use once a year to the Governing body.

Date of Incident	Description	Immediate corrective action	Further action	Legal implications	

Acceptable Use Agreement for Community Users

This Acceptable Use Agreement is intended to ensure:

- That community users of Cauldwell School's digital technologies will be responsible users and stay safe while using these systems and devices
- That Cauldwell School's systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- That users are protected from potential risk in their use of these systems and devices

Acceptable Use Agreement:

I understand that I must use Cauldwell School's systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school

- I understand that my use of school systems and devices and digital communications will be monitored
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- I will ensure that if I take and / or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
- I will not, without permission, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a school device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable or cause any damage to school / academy equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that if I fail to comply with this Acceptable Use Agreement, the school has the right to remove my access to school systems / devices
- I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Name

Signed

		Date	