

Online-Safety Policy

Schedule for Review and Development

This online-safety policy was reviewed by the Full Governing Body	July 2024
The implementation of this online safety policy will be monitored by the:	Online Safety Lead, The S.L.T and the School Council
The Online-safety Policy will be reviewed annually, 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:	March 2025
Should serious online-safety incidents take place, the following external persons / agencies should be informed as appropriate:	The LA Safeguarding Officer, Police.

Development of this Policy

This online safety policy has been developed by a working group made up of:

- Mr Wood – Headteacher, Online Safety lead (DSL)
- Mr Speirs – Assistant Headteacher (DSL)
- Staff – including Teachers, Support Staff, Technical staff
- Governors
- Parents and Carers
- The School Council

Consultation with the whole school community has taken place through a range of formal and informal meetings.

Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology.
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

Scope of the Policy

This policy applies to all members of the school community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school IT systems, both in and out of the school. Non-school based staff are subject to the County Council's IT Acceptable Use Policy.

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 incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate online-safety behaviour that take place out of school.

Roles and Responsibilities

Governors

Governors are responsible for the approval, monitoring and review of the Online-Safety Policy as well as for holding the Head Teacher to account for its implementation. This will be carried out by the Governors, receiving regular information about online-safety incidents and monitoring outcomes through the Headteacher's Report. The role of Online-Safety Governor is included within the role of the Safeguarding Governor and this part of their role will include:

- regular meetings with the Online-safety Lead
- discussion of online-safety incident logs
- reporting to relevant Governors meeting

All Governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix E)

Headteacher and Senior Leaders:

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

- The Headteacher has a duty of care for ensuring the safety (including online-safety) of members of the school community, though the day to day responsibility for online-safety will be delegated to the Online-safety Lead.
- The Headteacher and other Senior Designated Safeguarding officers are aware of the procedures to be followed in the event of a serious online-safety allegation being made against a member of staff as outlined on the flowchart later in this policy.
- The Headteacher and the Deputy Head Teacher are responsible for ensuring that the Online-safety Lead and other relevant staff receive suitable training to enable them to carry out their online-safety roles and to train other colleagues, as relevant.
- The Headteacher will 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.
- The Senior Leadership Team will receive regular monitoring reports from the Online-safety Lead.

Online-safety Lead:

Details of the school's safeguarding leads are set out in our child protection and safeguarding policy as well relevant job descriptions.

In our school, the Online Safety Lead takes lead responsibility for online safety in school through the following roles:

- takes day to day responsibility for online-safety issues and has a leading role in establishing and reviewing the school online-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online-safety incident taking place.
- Oversees the training for staff and gives advice
- liaises with the Local Authority / relevant body
- liaises with school technical staff
- consulting stakeholders – including parents / carers and the students / pupils about the online-safety provision
- receives reports of online-safety incidents and creates a log of incidents to inform future online-safety developments. Reports will be given via the safeguarding Pink form system and will be kept within the Safeguarding file
- meets regularly with Online-safety Governor, to discuss current issues, review incident logs
- attends relevant Governor meetings
- reports regularly to Senior Leadership Team

Network Support Services / IT Technician:

Our Network Support Provider along with our IT Technician are responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online-safety technical requirements and any Local Authority Online-safety Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy, is applied and updated on a regular basis (through GVITS)
- that they keep up to date with online-safety technical information to effectively carry out their online-safety role and to inform and update others as relevant

- that the use of the network is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher or the Online-safety Lead for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in school policies

All Staff and Volunteers

are responsible for ensuring that:

- they have an up to date awareness of online-safety matters and of the current school online-safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the Headteacher or the Online-safety Lead for investigation / action / sanction
- all digital communications with students / pupils / parents / carers should be on a professional level.
- online-safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the online-safety and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies about these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- working with the online-safety lead to ensure that any online safety incidents are logged (see appendix G) and dealt with appropriately and in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

Child Protection / Safeguarding Designated Persons

Our safeguarding senior designated persons are trained in online-safety issues and are aware of the potential for serious child protection / safeguarding 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
- cyber-bullying

Pupils:

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- 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

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents

understand these issues through parents' evenings, newsletters, letters, website, literature; likewise, we encourage parents to inform the school of any pertinent information that they come across that could affect the safety of children. Parents and carers will be encouraged to support the school in promoting good online-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website
- their comments on social media
- their children's personal devices in the school

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices A and/or B)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? - [UK Safer Internet Centre](#)
- Hot topics - [Childnet International](#)
- Parent factsheet - [Childnet International](#)

Community Users / Visitors

Community Users (including CRASH, Stagecoach and the Shelter Museum site) and visitors who wish to access any school systems or the website as part of the wider school provision will be made aware of this policy when relevant and expected to read and follow it. They will be expected to sign a Community User AUA before being provided with access to school systems.

Policy Statements

Education – pupils

The education of our *pupils* in online-safety is an essential part of the school's online-safety provision. Children and young people need the help and support of the school to recognise and avoid online-safety risks and build their resilience. The National Curriculum 2014 states that

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

Additionally, the requirements of the Relationships education and health education guidance 2020 are that by the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not.
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

Online-safety is a focus in all areas of the curriculum and staff reinforce online-safety messages across the curriculum. Our online-safety curriculum is broad, relevant and provides progression, with opportunities for creative activities and is provided in the following ways:

- A planned online-safety curriculum is provided as part of Computing / PHSE / other lessons and is revisited annually.
- Key online-safety messages are reinforced as part of a planned programme of assemblies and class-based sessions.
- Pupils are taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils are helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff act as good role models in their use of digital technologies the internet and mobile devices
- in lessons where internet use is pre-planned, pupils are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff are vigilant in monitoring the content of the websites the young people visit.

Education – parents / carers

We recognise that many parents and carers have only a limited understanding of online-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. We know that some parents underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site,
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

Education & Training – Staff / Volunteers

We recognise that it is essential that all staff receive online-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online-safety training needs of all staff will be carried out regularly.
- All new staff will receive online-safety training as part of their induction programme, ensuring that they fully understand the school online-safety policy and Acceptable Use Agreements.
- The Online-safety Lead will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This Online-safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The Online-safety Lead will provide advice / guidance / training to individuals as required.

Training – Governors

Governors will take part in online-safety training / awareness sessions. This will be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation.
- Participation in school training / information sessions for staff or parents.

Technical – infrastructure / equipment, filtering and monitoring

The school is responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will do this by:

- Managing our technical systems to ensure that the school meets recommended technical requirements.
- Making regular reviews and audits of the safety and security of school technical systems
- Locating Servers, wireless systems and cabling securely located and with restricted physical access. (IT Technicians room)
- Clearly defining access rights to school technical systems and devices for all users.
- Providing all users (at KS2 and above) with a username and maintaining an up to date record of users and their usernames.
- Ensuring that the “master / administrator” passwords for the school IT system, used by the Network Manager are also available to the Head teacher and kept in the school safe.
- Ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Filtering Internet access for all users. Illegal content is filtered by the broadband provider. Content lists are regularly updated by GVITS and internet use is logged and regularly monitored.
- The school has provided enhanced / differentiated user-level filtering.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach. This is, in the first instance to the IT Technician, who will log the incident and refer to the E Safety lead in an appropriate timescale.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- Having an agreed policy in place for the provision of temporary access of “guests” (eg trainee teachers, supply teachers, visitors) onto the school systems.
- We have an agreed policy in place regarding the extent of personal use that users (staff / students / pupils' / community users) and their family members are allowed on school devices that may be used out of school.
- In the course of normal operations, IT resources are to be used for business purposes only. The school permits limited personal use of IT facilities by authorised users subject to the following limitations:
 - Personal use must be in the user's own time and must not impact upon work efficiency or costs
 - The level of use must be reasonable and not detrimental to the main purpose for which the facilities are provided
 - Personal use must not be of a commercial or profit-making nature
 - Personal use must not be of a nature that competes with the business of the school or conflicts with an employee's obligations
- Personal use of the Internet must not involve attempting to access the categories of content described above that is normally automatically blocked by web filtering software.
- The Headteacher has delegated the right to make decisions to allow staff to download executable files and install programmes on school devices to the IT Technician and Coordinator.
- Staff will only use removable media (e.g. memory sticks / CDs / DVDs) on school devices if their use directly relates to school business and all necessary scans and checks will be carried out to minimise any transfer of viruses. Personal data will not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Use of digital and video images

We recognise that 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, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. We will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff will inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, we will stress the risks attached to publishing their own images on the internet e.g. on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, we allow parents / carers to take videos and digital images of their children at school events for their own personal use. To respect everyone's privacy and in some cases protection, all are reminded that these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images. Parental helpers will be asked not to take any photographs on school trips or when helping in school.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images are only taken on school equipment, the personal equipment of staff, parents or other volunteers are not to be used for such purposes.
- Care is taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils are not allowed to take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils are selected carefully and comply with good practice guidance on the use of such images.
- Pupils' full names are not used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers is obtained via a general consent form before photographs of pupils are published on the school website.
- Pupil's work is only published with the permission of the pupil and parents or carers.

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.

Please refer to the School's Data Protection Policy.

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

- the data must be encrypted and password protected
- the device must 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 policy (below) once it has been transferred or its use is complete

Communications

When using communication technologies, the school considers the following as good practice:

- The official school email service via the Gmail accounts ending @cliffordroad.suffolk.sch.uk may be regarded as safe and secure and is monitored. (Users should be aware that email communications are monitored.).
- Users must immediately report, to the nominated person (Online-Safety lead) – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents / carers (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 social media must not be used for these communications.
- Whole class / group email addresses may be used at KS1, while pupils at KS2 and above will be provided with individual school email addresses for educational use when needed
- Pupils should be taught about online-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Where Google domain is to be used to assist remote learning, parental consent will be gained prior to children being given access to their account. Parents are directed to <https://support.google.com/a/answer/6356509?hl=en> for more information on this.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training includes: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions.
- Risk assessment, including legal risk

School staff should ensure that they protect their professional reputation by ensuring that they use their personal accounts in an appropriate manner:

- Staff members need to use social networking in a way that does not conflict with the current National Teacher's Standards.
- Staff must never add pupils as friends into their personal accounts
- 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
- Staff must not post negative comments about the school, pupils, parents or colleagues including Governors.
- Staff must not post pictures of school events without the Headteacher's consent
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

At present the school has chosen not to use social media for professional purposes. Should this change care will be taken to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies. All social media services must be approved by the Headteacher in advance of any educational work being undertaken.

Parents and carers will be made aware of their responsibilities regarding their use of social networking. Methods of school communication include the prospectus, the website, newsletters, letters and verbal discussion.

- Parents should not post pictures of pupils other than their own children on social networking sites.

- Parents should make complaints through official school channels rather than posting them on social networking sites.
- Parents should not post malicious or fictitious comments on social networking sites about any member of the school community.

Remote Learning

At Clifford Road, we use Tapestry (in EYFS) and Google Classroom as our remote learning platforms. In the event of school closure (e.g. COVID-19) we make use of these platforms to deliver learning via digital means.

Our Remote Learning Rationale offers remote learning opportunities whilst also acknowledging that some households have limited access to devices and would require hard-copies of work and resources.

All stake-holders are expected to follow the guiding principles outlined in this online safety policy when working remotely.

There may be occasions when the school needs to implement and use video conferencing. We have created an online meeting guidelines, information and expectations letter, sent to all parents and available on our website (See Appendix M).

Cyber-bullying

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their classes and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, P4C and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The Online-Safety Lead will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or

- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the Online-Safety lead or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation. Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Unsuitable / inappropriate activities

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

The following actions are both unacceptable and illegal:

Visiting Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978
- Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003
- Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008
- criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986

The following actions are unacceptable:

Visiting Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- pornography
- promotion of any kind of discrimination
- 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

Any of the following actions:

- Using school systems to run a private business
- Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy
- Infringing copyright
- 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
- Unfair usage (downloading / uploading large files that hinders others in their use of the internet)

Responding to incidents of misuse

Incidents will be dealt with in line with the Suffolk County Council Flowchart – see appendix E

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.

Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
 - Internal response or discipline procedures
 - Involvement by Local Authority or national / local organisation (as relevant).
 - Police involvement and/or action
- **If content being reviewed includes images of Child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
 - incidents of 'grooming' behaviour
 - the sending of obscene materials to a child
 - adult material which potentially breaches the Obscene Publications Act
 - criminally racist material
 - other criminal conduct, activity or materials
- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions & Sanctions

If the school needs to deal with incidents that involve inappropriate rather than illegal misuse incidents will be dealt with as soon as possible in a proportionate manner, members of the school community will be made aware that the incidents have been dealt with. It is intended that incidents of misuse will be dealt with through our normal behaviour / disciplinary procedures.

Appendices

- A.** Student / Pupil Acceptable Use Agreement (older children)
- B.** Student / Pupil Acceptable Use Agreement (younger children)
- C.** Parent / Carer Information on our Acceptable Use Agreement
- D.** Use of Digital / Video Images
- E.** Staff, Governors and Volunteers Acceptable Use Agreement Policy
- F.** Community Users Acceptable Use Agreement
- G.** Responding to incidents of misuse – Suffolk County Council flowchart
- H.** Record of reviewing devices / internet sites (responding to incidents of misuse)
- I.** Legislation
- J.** Recording Form for Safeguarding Concerns
- K.** Parental consent for G Suite for Education Child Account.
- L.** G Suite for Education Notice to Parents and Guardians
- M.** Online Meeting Guidelines, Information and Expectations

Appendix A

KS2 Pupil/School using Digital Technology Agreement

School

Digital technologies have become important parts of all of our lives. They help us by stimulating discussion, helping us to be creative and to put some of our learning within the real world outside of Clifford Road. Because of this it is important that you have safe internet access at all times.

This agreement is to make sure that:

- that you will be responsible and stay safe while using the internet and other digital technologies for educational, personal use and whilst you are playing.
- that school systems and other users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to make sure that you will have good access to digital technologies to support you in your learning and will, in return, expect you to agree to be responsible users.

Pupil

I understand that I must be responsible when I am using school computing systems, so that there is no risk to my safety or to the safety and security of the computing systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of school equipment.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not give any personal information about myself or others when on-line (this includes names, addresses, email addresses, telephone numbers, age, what school I go to, etc)
- I will not arrange to meet people that I have only met on-line.
- If I see any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line I will minimise it on screen and immediately tell an adult.

I understand that everyone has equal rights to use technology and:

- I understand that the school systems and devices are there for educational use and that I will not use them for personal use or to play on unless I have permission.
- I will not try (unless I have permission) to make large downloads which may slow down the computers for others.
- I will not use the school systems or devices for playing games online, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not open, copy, remove or change anyone else's files, unless they know about it and have given their permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take a picture of anyone without their permission and I won't pass it on or post it on any sites.

I know that the school has to make sure that its technological equipment is looked after properly so

that the school can run smoothly:

- I will only use my own personal devices (mobile phones / USB devices etc) in school if I have permission. I understand that, if I do use my own devices in the school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or open up any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems.
- I will immediately report any damage or faults involving equipment or software, however it has happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation that sent the email.
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will only use social media sites with permission and that are appropriate for my age.

When using the internet for research or play, I recognise that:

- I should 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 try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (for example cyber-bullying, using other people's pictures or personal information).
- I understand that if I fail to comply with this agreement, there will be consequences. These may be the loss of access to the school network / internet, exclusions, contact with my parents and, if I do something illegal, involvement of the police.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the agreement. If you do not sign and return this agreement, we will not be able to use school systems and devices.

KS2 Pupil using Digital Technology Agreement

This form relates to the KS2 Pupil using Digital Technology Agreement, which it is attached.
Please complete the sections below to show that you have read, understood and agree to the rules included in this agreement. If you do not sign and return this agreement, you will not be able to use school IT systems and equipment.

I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)
- I use my own devices in the school (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc
- I use my own equipment out of the school in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school email, website etc.

Name of Pupil

Class

Signed

Date

Appendix B

Foundation/KS1 Pupil using Digital Technology Agreement

This is how we stay safe when we use computers:

I will ask a teacher or suitable adult if I want to use the computers

I will only use activities that a teacher or suitable adult has told or allowed me to use.

I will take care of the computers and other equipment.

I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.

If I see something that upsets me on the screen. I will minimise the screen and tell a teacher or suitable adult immediately.

I know that if I break the rules I might not be allowed to use the computers or other equipment.

Signed (child):.....

Signed (parent):

Appendix C

Parent / Carer Information on our Acceptable Use Agreement

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

The attached Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of online-safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will work hard to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect them to be responsible users. A copy of the Pupil Acceptable Use Policy is attached to this permission form, so that you will be aware of the school expectations of the children.

At Clifford Road Primary, we use G Suite for Education, and through this agreement, we are seeking your permission to provide and manage a G Suite for Education account for your child. G Suite for Education is a set of education productivity tools from Google including Gmail, Calendar, Docs, Classroom, and more, students may use their G Suite accounts to complete assignments, communicate with their teachers, and cover the digital literacy aspects of the National Curriculum.

We hope that you will support us in this important aspect of our work and feel that you can reinforce our messages at home, encouraging your child to adopt safe use of the internet and digital technologies at home and informing the school if you have concerns over your child's online-safety.

Teachers will be discussing the Acceptable Use Agreement and its meaning with your child and will continue to provide online-safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

At school we will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and IT systems but cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

Children's activity on our IT systems will be monitored and that the school will contact you if they have concerns about any possible breaches of the Acceptable Use Policy.

We will assume that parents are happy to give permission for their children to have access to the Internet and IT systems at school and that if this is not the case they will inform that school in writing of this. (Please address this instruction to the Headteacher.)

Appendix D

Use of Digital / Video Images

The use of digital / video images plays an important part in learning activities. Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media,

In order to comply with the Data Protection Act, we request your permission to take images of members of the school. We will ensure that when images are published that the young people cannot be identified by the use of their names.

In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.

Parents/carers will need to have signed and returned the permission form below before being able to take photos or video at school events

Digital / Video Images Permission Form

Parent / Carers Name

Pupil Name

As the parent / carer of the above pupil, I agree to the school taking and using digital / video images of my child / children. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school.

Yes / No

I agree that if I take digital or video images at, or of, – school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.

Yes / No

Signed

Date

Appendix E

Acceptable use agreement for staff, governors and volunteers

When using the schools' IT facilities and accessing the internet in school, or outside school on a work device, I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the schools' reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the schools' network
- Share my password with others or log in to the schools' network using someone else's details
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I am not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

I understand that the school will monitor the websites I visit and my use of the schools' IT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the schools' data protection policy.

I will let the Designated Safeguarding Lead (DSL) know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the schools' IT systems and internet responsibly and ensure that pupils in my care do so too.

Staff / Governor/ Volunteer Name

Signed

Date

Appendix F

Acceptable Use Agreement for Community Users

This Acceptable Use Agreement is intended to ensure:

- that community users of school digital technologies will be responsible users and stay safe while using these systems and devices
- that school 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 school 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 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 IT 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

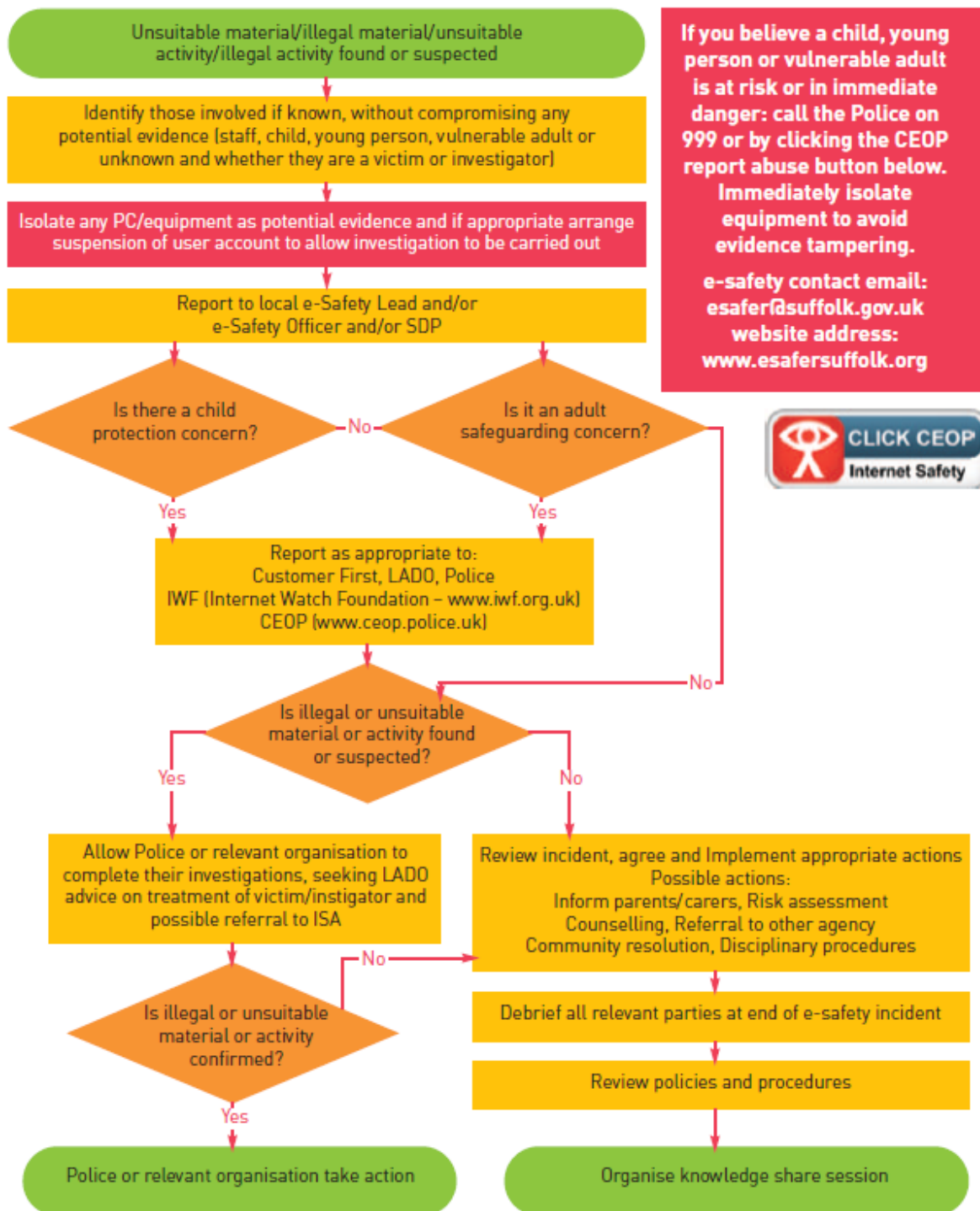
Signed

Date

Appendix G

Responding to incidents of misuse – flow chart

e-Safety Incident Flowchart



Appendix H

Clifford Road Primary School

Record of reviewing devices / internet sites (responding to incidents of misuse)

Group	
Date	
Reason for investigation	

Details of first reviewing person

Name	
Position	
Signature	

Details of second reviewing person

Name	
Position	
Signature	

Name and location of computer used for review (for web sites)

--

Web site(s) address / device

Reason for concern

Conclusion and Action proposed or taken

Appendix I

Legislation

The following legislation has been taken into account during the writing of this policy. It is assumed that an action that is illegal if committed offline is also illegal if committed online.

Legal advice may be sought in the advent of an e safety issue or situation.

Computer Misuse Act 1990

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.

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.

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.

Communications Act 2003

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.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

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.

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.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. youtube).

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.

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.

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.

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.

Sexual Offences Act 2003

The new grooming offence 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, connections staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

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. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

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.

The Education and Inspections Act 2006

Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data thus giving teachers stronger powers to tackle cyber-bullying.

<http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation>

The Protection of Freedoms Act 2012

Requires schools to seek permission from a parent / carer to use Biometric systems

The School Information Regulations 2012

Requires schools to publish certain information on its website:

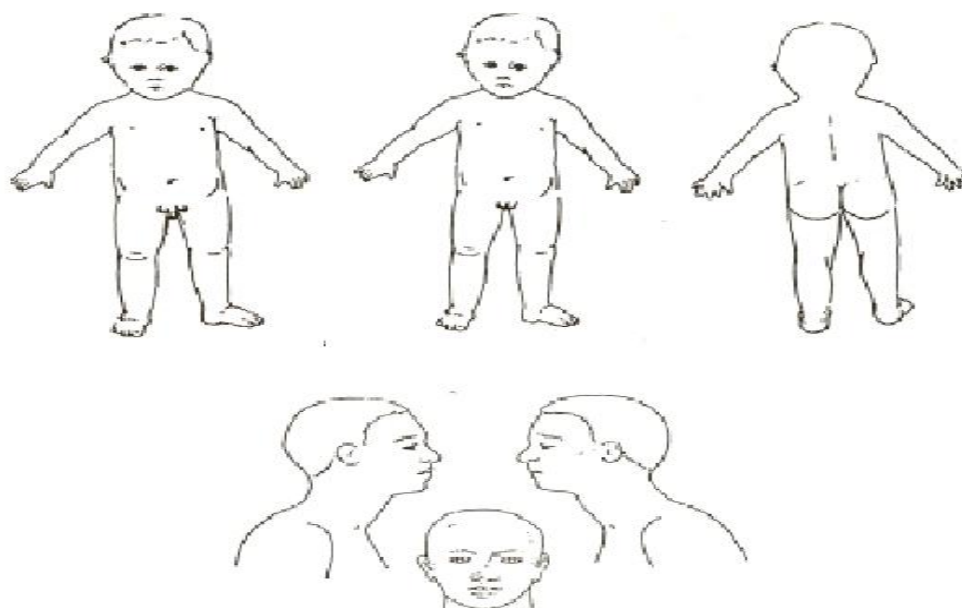
<http://www.education.gov.uk/schools/toolsandinitiatives/cuttingburdens/b0075738/reducing-bureaucracy/requirements/changeschoolinformationregulations>

Appendix J
Recording Form for Safeguarding Concerns
(Must be hand-written)

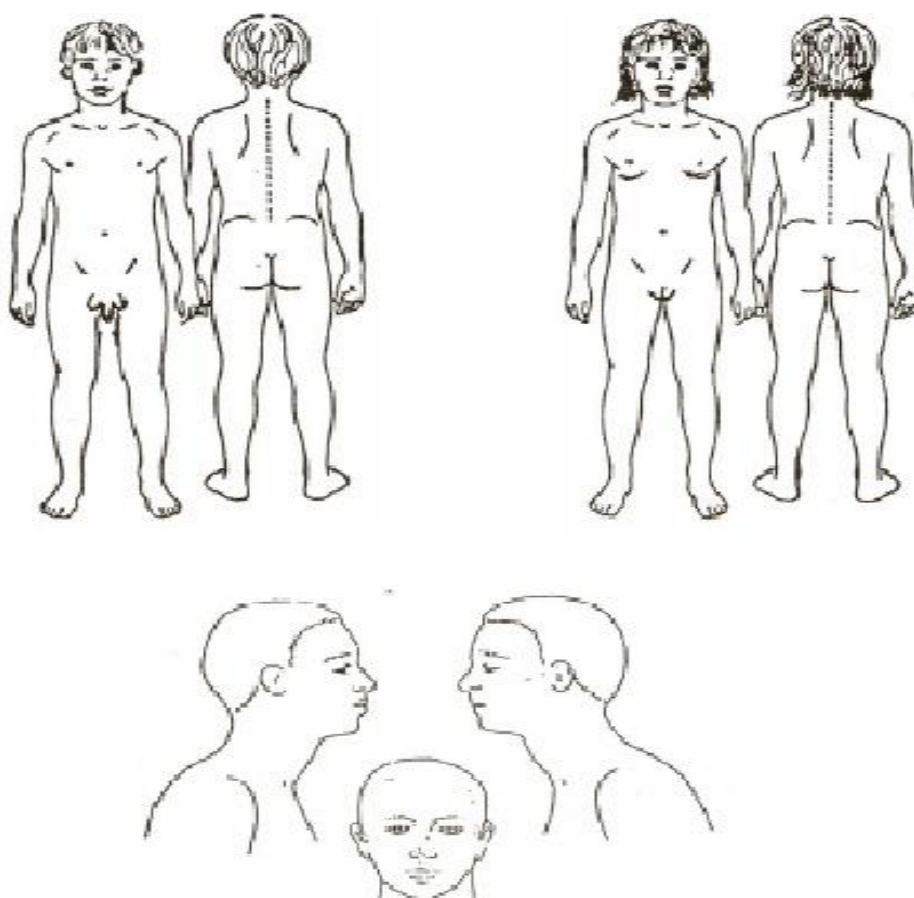
Name of pupil	Pupil's date of birth	Class	Your name (and position in school)

Nature of Concern/Disclosure (Remember to only record fact DO NOT add your own opinion)													
Was there an injury?	Yes		No		N/A		Did you see it?	Yes		No		N/A	
Describe the injury (if applicable):													
Have you filled in the body plan on the reverse of this form to show where the injury is and its approximate size?							Yes		No		N/A		
Was anyone else with you?	Yes		No		If yes, who?								
Where were you?													
Has this happened before?		Yes		No		When?							
Did you report the previous incident?		Yes		No		To Whom?					Date:		
Does the safeguarding concern involve a technological device?								Yes*		No			
*If yes, discuss this with your online-safety Lead: Jacqui Noon													
Who are you passing this information on to?													
Your Name:						Time:				Date:			
Signature of person receiving form:										Date received:			
Actions:													

Body map: Age 5 and under



Body map: Age 5 and over



Appendix K

Parental consent for G Suite for Education Child Account.

At Clifford Road Primary School, we use G Suite for Education, and seek your permission to provide and manage a G Suite for Education account for your child. G Suite for Education is a set of education productivity tools from Google including Gmail, Calendar, Docs, Classroom, and more. Your child will use their G Suite accounts to access a range of remote learning opportunities as well as communicating with their teachers.

The notice below provides answers to common questions about what Google can and can't do with your child's personal information, including:

- What personal information does Google collect?
- How does Google use this information?
- Will Google disclose my child's personal information?
- Does Google use student personal information for users in K-12 schools to target advertising?
- Can my child share information with others using the G Suite for Education account?

Please read it carefully, let us know of any questions, and then sign below to indicate that you've read the notice and give your consent. If you don't provide your consent, we will not create a G Suite for Education account for your child.

I give permission for Clifford Road Primary School to create/maintain a G Suite for Education account for my child and for Google to collect, use, and disclose information about my child only for the purposes described in the notice below.

Thank you,

Full name of student

Printed name of parent/carers

Signature of parent/carers

Date

Appendix L

G Suite for Education Notice to Parents and Guardians

This notice describes the personal information we provide to Google for these accounts and how Google collects, uses, and discloses personal information from students in connection with these accounts.

Using their G Suite for Education accounts, students may access and use the following "Core Services" offered by Google (described at https://gsuite.google.com/terms/user_features.html):

- Gmail
- Google+
- Calendar
- Chrome Sync
- Classroom
- Cloud Search
- Contacts
- Docs, Sheets, Slides, Forms
- Drive
- Groups
- Google Hangouts, Google Chat, Google Meet, Google Talk
- Jamboard
- Keep
- Sites
- Vault

Google provides information about the information it collects, as well as how it uses and discloses the information it collects from G Suite for Education accounts in its G Suite for Education Privacy Notice. You can read that notice online at https://gsuite.google.com/terms/education_privacy.html. You should review this information in its entirety, but below are answers to some common questions:

What personal information does Google collect?

When creating a student account, Clifford Road Primary School may provide Google with certain personal information about the student, including, for example, a name, email address, and password. Google may also collect personal information directly from students, such as telephone number for account recovery or a profile photo added to the G Suite for Education account.

When a student uses Google services, Google also collects information based on the use of those services. This includes:

- device information, such as the hardware model, operating system version, unique device identifiers, and mobile network information including phone number;
- log information, including details of how a user used Google services, device event information, and the user's Internet protocol (IP) address;
- location information, as determined by various technologies including IP address, GPS, and other sensors;
- unique application numbers, such as application version number; and
- cookies or similar technologies which are used to collect and store information about a browser or device, such as preferred language and other settings.

How does Google use this information?

In G Suite for Education Core Services, Google uses student personal information to provide, maintain, and protect the services. Google does not serve ads in the Core Services or use personal information collected in the Core Services for advertising purposes.

Can my child share information with others using the G Suite for Education account?

We may allow students to access Google services such as Google Docs and Sites, which include features where users can share information with others or publicly. When users share information publicly, it may be indexable by search engines, including Google.

Will Google disclose my child's personal information?

Google will not share personal information with companies, organizations and individuals outside of Google unless one of the following circumstances applies:

- With parental or guardian consent. Google will share personal information with companies, organizations or individuals outside of Google when it has parents' consent (for users below the age of consent), which may be obtained through G Suite for Education schools.
- With Clifford Road Primary School. G Suite for Education accounts, because they are school-managed accounts, give administrators access to information stored in them.
- For external processing. Google may provide personal information to affiliates or other trusted businesses or persons to process it for Google, based on Google's instructions and in compliance with the G Suite for Education privacy notice and any other appropriate confidentiality and security measures.
- For legal reasons. Google will share personal information with companies, organizations or individuals outside of Google if it has a good-faith belief that access, use, preservation or disclosure of the information is reasonably necessary to:
- meet any applicable law, regulation, legal process or enforceable governmental request.
- enforce applicable Terms of Service, including investigation of potential violations.
- detect, prevent, or otherwise address fraud, security or technical issues.
- protect against harm to the rights, property or safety of Google, Google users or the public as required or permitted by law.

Google also shares non-personal information -- such as trends about the use of its services -- publicly and with its partners.

What choices do I have as a parent or guardian?

First, you can consent to the collection and use of your child's information by Google. If you don't provide your consent, we will not create a G Suite for Education account for your child, and Google will not collect or use your child's information as described in this notice.

If you consent to your child's use of G Suite for Education, you can access or request deletion of your child's G Suite for Education account by contacting the school office. If you wish to stop any further collection or use of your child's information, you can request that we use the service controls available to limit your child's access to features or services, or delete your child's account entirely. You and your child can also visit <https://myaccount.google.com> while signed in to the G Suite for Education account to view and manage the personal information and settings of the account.

What if I have more questions or would like to read further?

If you have questions about our use of Google's G Suite for Education accounts or the choices available to you, please contact your child's teacher via the school office. If you want to learn more about how Google collects, uses, and discloses personal information to provide services to us, please review the G Suite for Education Privacy Center (at <https://www.google.com/edu/trust/>), the G Suite for Education Privacy Notice (at https://gsuite.google.com/terms/education_privacy.html), and the Google Privacy Policy (at <https://www.google.com/intl/en/policies/privacy/>).

The Core G Suite for Education services are provided to us under Google's Apps for Education agreement (at https://www.google.com/apps/intl/en/terms/education_terms.html).

Appendix M

Clifford Road Primary School Online Meeting Guidelines, Information and Expectations

At Clifford Road Primary School, we deliver our remote learning provision through the use of Tapestry and Google Classroom.

There is no requirement for our teachers to run live lessons and staff are proactive in providing learning opportunities through recorded content, voice-over/screen casting and posted assignments.

However, at times, staff may make use of live video sessions for wellbeing, class cohesion/social discussion or enrichment opportunities. This will take place using Zoom, following all guidelines and rules that comply with our Safeguarding and Data Protection Policies.

When a member of staff sends an invitation to a Zoom meeting for your child, it will be password protected and monitored throughout.

Staff Expectations

- Two members of staff are required to run a Zoom session.
- The sessions may be recorded for the safeguarding of all. A Waiting Room should be available for participants before the meeting is ready to start. 'Chat' may be disabled depending on the purpose of the meeting.
- The meeting will be restricted to invited members only.
- Pupils will be reminded at the start of the session that there are clear expectations of all and they adhere to the school behaviour policy as they would in school normally.
- Staff will wear suitable clothing. The background scene should be appropriate.
- Staff should ensure that all members are muted when instructions are given.
- All Safeguarding concerns must be raised with the Designated Safeguarding Lead in school. The session may be stopped early if there are immediate concerns.

Parent Expectations

- Parents' consent to their child/children being part of the Zoom session and agree not to make any recordings or take photographs at any time.
- The child's login name should be their first name and just the initial letter of their surname. Staff need to identify pupils clearly. Zoom is not intended for use by individuals under the age of 16 unless it is through a session organised by the school.
- The content of each session is confidential as are the password and invitation codes.
- A parent must supervise their child during the session but will not be required to actively take part or be on screen. Other members of the household should also not be visible or audible.
- Parents must dress in appropriate clothing and use appropriate language when part of the session.
- Parents should not interact with the session but may contact the teacher after the session if there are any questions or concerns.
- Parents should ensure that the pupils are aware of the Pupil expectations set out below.

Pupil Expectations

- Pupils should be dressed appropriately in front of a suitable background.
- Pupils should not be taking part from their bedroom. Please ensure that the meeting takes place in a communal area of your household.
- Pupils must be aware of the school rules and understand that they need to behave sensibly, using polite language. Any child who does not comply with these rules may be removed from the session.
- Pupils should be aware that their voices will sometimes be muted and at other times they will be invited to speak. Pupils should keep their microphone muted when they are not asked to contribute.

We are looking forward to working with the children via Zoom and hope that the opportunity to come together virtually, is happy and safe for all. If you have any questions, please contact the school for more information