Moss Hall Schools Federation

Online Policy

Spring 2020

Last updated: Autumn 2020
Ratified by Full Governing Body: Autumn 2020
Next Review: Autumn 2021 (Annual review: statutory policy)

Contents

Moss Hall Federation Schools understands that using online services is an important aspect of raising educational standards, promoting pupil achievement and enhancing teaching and learning.

The use of online services is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of pupils and staff.

The breadth of issues classified within online safety is considerable, but they can be categorised into three areas of risk:

- **Content**: Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, and racist or radical and extremist views.

- **Contact**: Being subjected to harmful online interaction with other users, e.g. commercial advertising and adults posing as children or young adults.
- **Conduct**: Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.

The measures implemented to protect pupils and staff revolve around these areas of risk. Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

Signed by:

____________________ Executive Headteacher Date: ____________________

____________________ Chair of governors Date: ____________________

1. Legal framework

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Voyeurism (Offences) Act 2019
- The General Data Protection Regulation (GDPR)
- Data Protection Act 2018
- DfE (2020) 'Keeping children safe in education'
- DfE (2019) 'Teaching online safety in school'
- DfE (2018) 'Searching, screening and confiscation'
- National Cyber Security Centre (2017) 'Cyber Security: Small Business Guide'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'
- UK Council for Child Internet Safety (2017) 'Sexting in schools and colleges: Responding to incidents and safeguarding young people'

This policy operates in conjunction with the following school policies:

- **Acceptable Use Agreement**
- **Child Protection and Safeguarding Policy**
- **Anti-Bullying Policy**
- **PSHE Policy**
- **RSE and Health Education Policy**
- **Staff Code of Conduct**
- **Behavioural Policy**
- **Disciplinary Policy and Procedures**
- **Data Protection Policy**
- **User Agreement**
- **Prevent Duty Policy**
- **Pupil Remote Learning Policy**

2. Roles and responsibilities

The **governing board** is responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the DSL's remit covers online safety.
- Reviewing this policy on an **annual** basis.
- Ensuring their own knowledge of online safety issues is up-to-date.
- Ensuring all staff undergo safeguarding and child protection training (including online safety) at induction.
- Ensuring that there are appropriate filtering and monitoring systems in place.

The **Executive Executive Headteacher** is responsible for:

- Supporting the DSL and any deputies by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.

- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated.
- Supporting staff to ensure that online safety is embedded throughout the curriculum so that all pupils can develop an appropriate understanding of online safety.
- Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping pupils safe.
- Working with the **DSL and governing board** to update this policy on an **annual** basis.

The DSL is responsible for:

- Taking the lead responsibility for online safety in the school.
- Acting as the named point of contact within the school on all online safeguarding issues.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.
- Liaising with relevant members of staff on online safety matters, e.g. the SENCO and ICT technicians.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the school's approach to remote learning.
- Ensuring appropriate referrals are made to external agencies, as required.
- Staying up-to-date with current research, legislation and online trends.
- Coordinating the school's participation in local and national online safety events, e.g. Safer Internet Day.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff.
- Ensuring all members of the school community understand the reporting procedure.
- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.
- Monitoring online safety incidents to identify trends and any gaps in the school's provision, and using this data to update the school's procedures.
- Reporting to the **governing board** about online safety on a **termly** basis.
- Working with the **Executive Headteacher and governing board** to update this policy on an **annual** basis.

ICT technicians are responsible for:

- Providing technical support in the development and implementation of the school's online safety policies and procedures.
- Implementing appropriate security measures as directed by the **Executive Executive Headteacher**.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.
- Working with the **DSL and Executive Headteacher** to conduct **half-termly** light-touch reviews of this policy.

All staff members are responsible for:

- Taking responsibility for the security of ICT systems and electronic data they use or have access to.
- Modelling good online behaviours.
- Maintaining a professional level of conduct in their personal use of technology.
- Having an awareness of online safety issues.
- Reporting concerns in line with the school's reporting procedure.

- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

Pupils are responsible for:

- Adhering to this policy, the **Acceptable Use Agreement** and other relevant policies.
- Seeking help from school staff if they are concerned about something they or a peer has experienced online.
- Reporting online safety incidents and concerns in line with the procedures within this policy.

3. The curriculum

Online safety is embedded throughout the curriculum

The curriculum and the school's approach to online safety is developed in line with the UK Council for Child Internet Safety's 'Education for a Connected World' framework and the DfE's 'Teaching online safety in school' guidance. https://www.gov.uk/government/publications/teaching-online-safety-in-schools

Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using.

Online safety teaching is always appropriate to pupils' ages and developmental stages. The underpinning knowledge and behaviours pupils learn through the curriculum include the following

- How to evaluate what they see online
- How to recognise techniques used for persuasion
- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support

The online risks pupils may face online are always considered when developing the curriculum. The risks that are considered and how they are covered in the curriculum can be found in Appendix 1 of this policy.

The DSL is involved with the development of the school's online safety curriculum. The school recognises that, while any pupil can be vulnerable online, there are some pupils who may be more susceptible to online harm or have less support from family and friends in staying safe online, e.g. pupils with SEND and LAC. Relevant members of staff, e.g. the SENCO and designated teacher for LAC, work together to ensure the curriculum is tailored so these pupils receive the information and support they need.

Class teachers review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils. When reviewing these resources, the following questions are asked:

- Where does this organisation get their information from?
- What is their evidence base?
- Have they been externally quality assured?
- What is their background?
- Are they age appropriate for pupils?

- Are they appropriate for pupils' developmental stage?

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The **Executive Headteacher and DSL** decide when it is appropriate to invite external groups into school and ensure the visitors selected are appropriate.

Before conducting a lesson or activity on online safety, the class teacher and DSL consider the topic that is being covered and the potential that pupils in the class have suffered or may be suffering from online abuse or harm in this way. The DSL advises the staff member on how to best support any pupil who may be especially impacted by a lesson or activity.

Lessons and activities are planned carefully so they do not draw attention to a pupil who is being or has been abused or harmed online, to avoid publicising the abuse.

During an online safety lesson or activity, the class teacher ensures a safe environment is maintained in which pupils feel comfortable to say what they feel and are not worried about getting into trouble or being judged.

If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will make a report in line with sections 15 and 16 of this policy.

If a pupil makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member will follow the reporting procedure outlined in sections 15 and 16 of this policy.

4. Staff training

All staff receive safeguarding and child protection training, which includes online safety training, during their induction.

Online safety training for staff is updated **annually** and is delivered in line with advice from the three local safeguarding partners.

In addition to this training, staff also receive regular online safety updates as required and at least annually.

The DSL and any deputies undergo training to provide them with the knowledge and skills they need to carry out their role, this includes online safety training. This training is updated at least every two years.

In addition to this formal training, the DSL and any deputies receive regular online safety updates to allow them to keep up with any developments relevant to their role. In relation to online safety, these updates allow the DSL and their deputies to:

- Understand the unique risks associated with online safety and be confident that they have the relevant knowledge and capability required to keep pupils safe while they are online at school.
- Recognise the additional risks that pupils with SEND face online and offer them support to stay safe online.

All staff are emailed a copy of this policy upon their induction and are informed of any changes to the policy.

Staff are required to adhere to the **Staff Code of Conduct** at all times, which includes provisions for the acceptable use of technologies and the use of social media.

All staff are informed about how to report online safety concerns, in line with sections 15 and 16 of this policy.

The DSL acts as the first point of contact for staff requiring advice about online safety.

5. Educating parents

The school works in partnership with parents to ensure pupils stay safe online at school and at home.

Parents are provided with information about the school's approach to online safety and their role in protecting their children. Parental awareness is raised in the following ways:

- Parents' evenings
- Twilight training sessions
- Newsletters

Parents are sent a copy of the **Acceptable Use Agreement** at **the beginning of each academic year** and are encouraged to go through this with their child to ensure their child understands the document and the implications of not following it.

6. Classroom use

A wide range of technology is used during lessons, including the following:

- Computers
- Laptops
- Tablets
- Internet
- Email
- Cameras
- Visualisers

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that pupils use these platforms at home, the class teacher always reviews and evaluates the resource.

Pupils are supervised when using online materials during lesson time – this supervision is suitable to their age and ability.

7. Internet access

Pupils, staff and other members of the school community are only granted access to the school's internet network once they have read and signed the **Acceptable Use Agreement**.

A record is kept of users who have been granted internet access in **the school office and shared area.**

All members of the school community are encouraged to use the school's internet network, instead of 3G, 4G and 5G networks, as the network has appropriate filtering and monitoring to ensure individuals are using the internet appropriately.

8. Filtering and monitoring online activity

The **governing board** ensures the school's ICT network has appropriate filters and monitoring systems in place.

The **Executive Headteacher and ICT technicians** undertake a risk assessment to determine what filtering and monitoring systems are required.

The **governing board** ensures 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

ICT technicians undertake **monthly** checks on the filtering and monitoring systems to ensure they are effective and appropriate.

Requests regarding making changes to the filtering system are directed to the **Executive Headteacher**.

Prior to making any changes to the filtering system, **ICT technicians and the DSL** conduct a risk assessment. Any changes made to the system are recorded by **ICT technicians**.

Reports of inappropriate websites or materials are made to **an ICT technician** immediately, who investigates the matter and makes any necessary changes.

Deliberate breaches of the filtering system are reported to **the DSL and ICT technicians**, who will escalate the matter appropriately.

If a pupil has deliberately breached the filtering system, they will be disciplined in line with the **Behaviour Policy**.

If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the **Disciplinary Policy and Procedure**.

If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g. the Internet Watch Foundation (IWF), CEOP and/or the police.

The school's network and school-owned devices are appropriately monitored by computing **co-ordinator or ICT technicians.**

Concerns identified through monitoring are reported to the **DSL** who manages the situation in line with sections 15 and 16 of this policy.

9. Network security

Technical security features, such as anti-virus software, are kept up-to-date and managed by **ICT technicians**. Firewalls are switched on at all times. **ICT technicians** review the firewalls on a **weekly** basis to ensure they are running correctly, and to carry out any required updates.

Staff and pupils are advised not to download unapproved software or open unfamiliar email attachments.

All members of staff have their own unique usernames and private passwords to access the school's systems. Pupils in **class year** and above are provided with their own unique username and private passwords. Staff members and pupils are responsible for keeping their passwords private. Passwords have a minimum and maximum length and require a mixture of letters, numbers and symbols to ensure they are as secure as possible. Passwords should be systematically changed regularly

Users are not permitted to share their login details with others and are not allowed to log in as another user at any time. Users are required to lock access to devices and systems when they are not in use. Users inform **Computing Co-Ordinator** or **ICT technicians** if they forget their login details, who will arrange for the user to access the systems under different login details.

If a user is found to be sharing their login details or otherwise mistreating the password system, the **Executive Headteacher** is informed and decides the necessary action to take.

10. Emails

Access to and the use of emails is managed in line with the **Data Protection Policy** and **Acceptable Use Agreement**.

Staff and pupils are given approved school email accounts and are only able to use these accounts at school and when doing school-related work outside of school hours.

Prior to being authorised to use the email system, staff and pupils must agree to and sign the relevant acceptable use agreement.

Personal email accounts are not permitted to be used on the school site.

Any email that contains sensitive or personal information is only sent using secure and encrypted email.

The school's monitoring system can detect inappropriate links, malware and profanity within emails – staff and pupils are made aware of this.

Chain letters, spam and all other emails from unknown sources are deleted without being opened.

Computing Co-ordinator organise an **annual** assembly where they explain what a phishing email and other malicious emails might look like – this assembly includes information on the following:

- How to determine whether an email address is legitimate
- The types of address a phishing email could use
- The importance of asking "does the email urge you to act immediately?"
- The importance of checking the spelling and grammar of an email

11. Social networking

Personal use

Access to social networking sites is filtered as appropriate.

Staff and pupils are not permitted to use social media for personal use during lesson time.

Staff can use personal social media during break and lunchtimes; however, inappropriate or excessive use of personal social media during school hours may result in the removal of internet access or further action.

Staff members are advised that their conduct on social media can have an impact on their role and reputation within the school.

Staff receive **annual** training on how to use social media safely and responsibly.

Staff are not permitted to communicate with pupils or parents over social networking sites and are reminded to alter their privacy settings to ensure pupils and parents are not able to contact them on social media.

Pupils are taught how to use social media safely and responsibly through the online safety curriculum.

Concerns regarding the online conduct of any member of the school community on social media are reported to the **DSL** and managed in accordance with the relevant policy, e.g. **Anti-Bullying Policy, Staff Code of Conduct and Behaviour Policy**.

Use on behalf of the school

The use of social media on behalf of the school is conducted in line with the **Social Media Policy**.

The school's official social media channels are only used for official educational or engagement purposes.

Staff members must be authorised by the **Executive Headteacher** to access to the school's social media accounts.

All communication on official social media channels by staff on behalf of the school is clear, transparent and open to scrutiny.

The **Staff Code of Conduct** contains information on the acceptable use of social media – staff members are required to follow these expectations at all times.

12. The school website

The **Executive Headteacher** is responsible for the overall content of the school website – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements.

The website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright law.

Personal information relating to staff and pupils is not published on the website.

Images and videos are only posted on the website if the provisions with School Policy are met.

13. Use of school-owned devices

Staff members are issued with the following devices to assist with their work:

- Laptop
- Chrome Book
- Ipad

Pupils are provided with school-owned devices as necessary to assist in the delivery of the curriculum, e.g. tablets to use during lessons. School-owned devices are used in accordance with the **User Agreement**.

Staff and pupils are not permitted to connect school-owned devices to public Wi-Fi networks.

All school-owned devices are password protected.

All mobile school-owned devices are fitted with tracking software to ensure they can be retrieved if lost or stolen.

All school-owned devices are fitted with software to ensure they can be remotely accessed, in case data on the device needs to be protected, retrieved or erased.

ICT technicians review all school-owned devices on a **Termly** basis to carry out software updates and ensure there is no inappropriate material on the devices.

No software, apps or other programmes can be downloaded onto a device without authorisation from **ICT technicians**.

Staff members or pupils found to be misusing school-owned devices are disciplined in line with the **Disciplinary Policy and Procedure** and **Behaviour Policy**.

14. Use of personal devices

Personal devices are used in accordance with School Policy.

Any personal electronic device that is brought into school is the responsibility of the user.

Personal devices are not permitted to be used in the following locations:

- Toilets
- Changing rooms
- Playground

Staff members are not permitted to use their personal devices during lesson time.

Staff members are not permitted to use their personal devices to take photos or videos of pupils.

14.1. Staff members report concerns about their colleagues' use of personal devices on the school premises in line with the **Disciplinary Policy and Procedures**

14.2. If a member of staff is thought to have illegal content saved or stored on a personal device, or to have committed an offence using a personal device, the **Executive Headteacher** will inform the police and action will be taken in line with the **Disciplinary Policy and Procedures**

Pupils are not permitted to use their personal devices during lesson time or when moving between lessons.

If a pupil needs to contact their parents during the school day, they are allowed to use the phone in the **school office**.

The **Executive Headteacher** may authorise the use of mobile devices by a pupil for safety or precautionary use.

If a staff member reasonably believes a pupil's personal device has been used to commit an offence or may provide evidence relating to an offence, the device will be handed to the police.

Appropriate signage is displayed to inform visitors to the school of the expected use of personal devices.

Any concerns about visitors' use of personal devices on the school premises are reported to the **DSL**.

15. Managing reports of online safety incidents

Staff members and pupils are informed about what constitutes inappropriate online behaviour in the following ways:

- Staff training
- The online safety curriculum
- Assemblies

Concerns regarding a staff member's online behaviour are reported to the **Executive Headteacher** who decides on the best course of action in line with the relevant policies, e.g. **Staff Code of Conduct and Disciplinary Policy and Procedures**.

Concerns regarding a pupil's online behaviour are reported to the **DSL** who investigates concerns with relevant staff members, e.g. **the Executive Headteacher and ICT technicians**.

Concerns regarding a pupil's online behaviour are dealt with in accordance with relevant policies depending on their nature, e.g. **Behaviour Policy and Child Protection and Safeguarding Policy**.

Where there is a concern that illegal activity has taken place, the **Executive Headteacher** contacts the police.

All online safety incidents and the school's response are recorded by the **DSL**.

16. Responding to specific online safety concerns

Cyberbullying

Cyberbullying, against both pupils and staff, is not tolerated.

Any incidents of cyberbullying are dealt with quickly and effectively whenever they occur.

Online sexual violence and sexual harassment between children (peer-on-peer abuse)

The school recognises that peer-on-peer abuse can take place online. Examples include the following:

- Non-consensual sharing of sexual images and videos
- Sexualised cyberbullying
- Online coercion and threats
- Unwanted sexual comments and messages on social media
- Online sexual exploitation

The school responds to all concerns regarding online peer-on-peer abuse, whether or not the incident took place on the school premises or using school-owned equipment.

Concerns regarding online peer-on-peer abuse are reported to the **DSL** who will investigate the matter in line with the **Child Protection and Safeguarding Policy**.

Information about the school's full response to incidents of online peer-on-peer abuse can be found in the **Child Protection and Safeguarding Policy**.

Upskirting

Under the Voyeurism (Offences) Act 2019, it is an offence to operate equipment and to record an image beneath a person's clothing without consent and with the intention of observing, or enabling another person to observe, the victim's genitals or buttocks (whether exposed or covered with underwear), in circumstances where their genitals, buttocks or underwear would not otherwise be visible, for a specified purpose.

A "specified purpose" is namely:

- Obtaining sexual gratification (either for themselves or for the person they are enabling to view the victim's genitals, buttocks or underwear).
- To humiliate, distress or alarm the victim.

"Operating equipment" includes enabling, or securing, activation by another person without that person's knowledge, e.g. a motion activated camera.

Upskirting is not tolerated by the school. Incidents of upskirting are reported to the **DSL** who will then decide on the next steps to take, which may include police involvement, in line with the **Child Protection and Safeguarding Policy**.

Youth produced sexual imagery (sexting)

Youth produced sexual imagery is the sending or posting of sexually suggestive images of under-18s via mobile phones or over the internet. Creating and sharing sexual photos and videos of individuals under 18 is illegal.

All concerns regarding sexting are reported to the **DSL**.

Online abuse and exploitation

Through the online safety curriculum, pupils are taught about how to recognise online abuse and where they can go for support if they experience it.

The school responds to concerns regarding online abuse and exploitation, whether or not it took place on the school premises or using school-owned equipment.

All concerns relating to online abuse and exploitation, including child sexual abuse and exploitation and criminal exploitation, are reported to the **DSL** and dealt with in line with the **Child Protection and Safeguarding Policy**.

Online hate

The school does not tolerate online hate content directed towards or posted by members of the school community.

Incidents of online hate are dealt with in line with the relevant school policy depending on the nature of the incident and those involved, e.g. **Staff Code of Conduct, Anti-Bullying Policy etc**

Online radicalisation and extremism

The school's filtering system protects pupils and staff from viewing extremist content.

Concerns regarding a staff member or pupil being radicalised online are dealt with in line with the **Child Protection and Safeguarding Policy** and **Prevent Duty Policy**.

17. Remote learning

All remote learning is delivered in line with the school's **Pupil Remote Learning Policy**.

All staff and pupils using video communication must:

- Communicate in groups – one-to-one sessions are only carried out where necessary.
- Wear suitable clothing – this includes others in their household.
- Be situated in a suitable 'public' living area within the home with an appropriate background – 'private' living areas within the home, such as bedrooms, are not permitted during video communication.
- Use appropriate language – this includes others in their household.
- Maintain the standard of behaviour expected in school.
- Use the necessary equipment and computer programs as intended.
- Not record, store, or distribute video material without permission.
- Ensure they have a stable connection to avoid disruption to lessons.
- Always remain aware that they are visible.

The school will consider whether one-to-one sessions are appropriate in some circumstances, e.g. to provide support for pupils with SEND. This will be decided and approved by the **SLT**, in collaboration with the **SENCO**.

Pupils not using devices or software as intended will be disciplined in line with the **Behaviour Policy**.

The school will consult with parents prior to the period of remote learning about what methods of delivering remote teaching are most suitable – alternate arrangements will be made where necessary.

The school will ensure that all school-owned equipment and technology used for remote learning has suitable anti-virus software installed, can establish secure connections, can recover lost work, and allows for audio and visual material to be recorded or downloaded, where required.

The school will communicate to parents in writing about any precautionary measures that need to be put in place if their child is learning remotely using their own/family-owned equipment and technology, e.g. ensuring that their internet connection is secure.

During the period of remote learning, the school will maintain regular contact with parents to:

- Reinforce the importance of children staying safe online.
- Ensure parents are aware of what their children are being asked to do, e.g. sites they have been asked to use and staff they will interact with.
- Encourage them to set age-appropriate parental controls on devices and internet filters to block malicious websites.
- Direct parents to useful resources to help them keep their children safe online.

The school will not be responsible for providing access to the internet off the school premises and will not be responsible for providing online safety software, e.g. anti-virus software, on devices not owned by the school.

18. Monitoring and review

The school recognises that the online world is constantly changing; therefore, **the DSL, ICT technicians and the Executive Headteacher** conduct **half-termly** light-touch reviews of this policy to evaluate its effectiveness.

The **governing board, Executive Headteacher and DSL** review this policy in full on an **annual** basis and following any online safety incidents.

The next scheduled review date for this policy is Autumn 2021.

Any changes made to this policy are communicated to all members of the school community

Keeping Safe: Stop, Think, Before you Click!

12 rules for responsible ICT use

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

1. I will only use the school's computers for schoolwork and homework.
2. I will only edit or delete my own files and not look at, or change, other people's files without their permission.
3. I will keep my logins and passwords secret.
4. I will not bring files into school without permission or upload inappropriate material to my workspace.
5. I am aware that some websites and social networks have age restrictions and I should respect this.
6. I will not attempt to visit Internet sites that I know to be banned by the school.
7. I will only e-mail people I know, or a responsible adult has approved.
8. The messages I send, or information I upload, will always be polite and sensible.
9. I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
10. I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission.
11. I will never arrange to meet someone I have only ever previously met on the Inter net, unless my parent/carer has given me permission and I take a responsible adult with me.
12. If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will show a teacher / responsible adult.

Pupil name: ____

I have read the school 'rules for responsible ICT use'. My parent / carer and teacher has explained them to me.

I understand these rules are there to help keep me safe, and my friends and family safe. I agree to follow the rules.

This means I will use the computers, Internet, e-mail, online communities, digital cameras, video recorders, and other ICT in a safe and responsible way.

I understand that the school can check my computer files, and the Internet sites I visit, and that if they have concerns about my safety, that they may contact my parent / guardian.

Pupil's signature: ______________________________________