Cleves School
Learning Together

E-SAFETY POLICY

Reviewed on	December 2021
Reviewed by	Hugh Thomas
Review Cycle	Annual
Next Review Date	December 2022

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and trustees
- 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

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff

It also refers to the Department's guidance on protecting children from radicalisation.
It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

This policy complies with our funding agreement and articles of association.

3. Roles and responsibilities

3.1 Responsibilities

The Cleves E-safety Policy is part of the Strategic Plan and relates to other policies including those for ICT, Behaviour, Anti-Bullying and Safeguarding. Hugh Thomas is the Cleves ICT Coordinator and Ian Russ is the Child Protection Coordinator. The E-Safety Coordinator is Craig Smith.
The Trustee who oversees online safety is Alistair Nelson

All trustees will:

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

3.2 The headteacher

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

3.3 The designated safeguarding lead
Details of the school's DSL (and deputies) are set out in our child protection and safeguarding policy as well relevant job descriptions.

The Deputy Headteacher takes lead responsibility for online safety at Cleves, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school's behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or Trustees

3.4 The Leadership Team and IT Support Company
The Leadership Team and IT Support Company are responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school's behaviour policy

3.5 All staff and volunteers
All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on the acceptable use of the school's ICT systems and the internet and ensuring that pupils follow the school's terms on acceptable use.
- Working with the DSL and Deputy Headteacher to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school's behaviour policy

3.6 Parents
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 1 and 2)
- 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

3.7 Visitors and members of the community
Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it.

4. Educating pupils about online safety

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole.

As E-safety is an important aspect of strategic leadership within the school, the Head and trustees have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named E-safety co-ordinator in this school is Craig Smith who has been designated this role as a member of the senior leadership team. All members of the school community have been made aware of who holds this post. It is the role of the E-safety co-ordinator to keep abreast of current issues and guidance.

Senior Management and Trustees are updated by the Head/E-safety co-ordinator and all trustees have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreement is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home–school agreements, and behaviour/pupil discipline (including the anti-bullying) policy and PSHE.

Pupils will be taught about online safety as part of the curriculum:

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

By the end of primary school, pupils will know:

- Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.
- Pupils are made aware of the implications of sharing images on social media and messaging platforms.
- Pupils are taught about the importance of checking privacy settings regularly on media platforms to ensure that their content is only available to the intended audience.
- Pupils are aware that they create digital footprints when using the internet/media platforms and the impact that a positive/negative history could have.
- Pupils are taught about copyright and respecting other people's information, images, etc through discussion, modeling and activities.
- Pupils are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline or CEOP report abuse button. (Anti-Bullying Policy - Section Cyber Bullying)
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum.
- Pupils are taught about the potential risks posed by communicating with other people online (and the possibility they may not be who they say).

The safe use of social media and the internet will also be covered in other subjects where relevant.

We will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

Whilst exciting and beneficial both in and out of the context of education, ICT, particularly web- based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Cleves School, we understand the responsibility to educate our pupils on eSafety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in newsletters or other communications home, and in information via our website.

Online safety will also be covered during curriculum evenings for parents.
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.

6. Cyber-bullying

6.1 Definition
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.

6.2 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. Staff will discuss cyber-bullying with pupils, 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, and other subjects where appropriate.

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

The academy 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 academy will follow the processes set out in the behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the academy will use all reasonable endeavours to ensure the incident is contained.
The DSL 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
Academy 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 DSL 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.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and trustees are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

7.1 Monitoring

Authorised ICT staff may inspect any ICT equipment owned or leased by the School at any time without prior notice. ICT authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain School business related information; to confirm or investigate compliance with School policies, standards and procedures; to ensure the effective operation of School ICT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime.

ICT authorised staff may, without prior notice, access the e-mail or voice-mail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

The school's ICT systems security will be reviewed regularly. Virus protection will be updated regularly by the Network Manager and security strategies will be discussed with Senior Management, ICT Coordinator and ICT support agencies. Forensic Software is in use and will monitor pupil's use of a computer in accordance with the Acceptable Use Policy. In line with recommended guidelines, filters and monitoring systems are in place to limit pupils' exposure to risks associated with technology such as:

- Child sexual exploitation
- Radicalisation
- Sexual predation
- Cyber-bullying

Any inappropriate usage will be reported to the designated safeguarding leads.

7.2 Computer Viruses

All files downloaded from the Internet, received via e-mail or on removable media (e.g. memory stick, CD) must be checked for any viruses using school provided anti-virus software before using them.

Never interfere with any anti-virus software installed on school ICT equipment that you use. If your machine is not routinely connected to the school network, you must make provision for regular virus updates through the ICT team.

If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact the School Business Manager or Deputy Headteacher immediately. They will advise you what actions to take and be responsible for advising others that need to know.

7.3 e-Mail and Google Hub

The use of e-mail within most schools is an essential means of communication for both staff and pupils. Educationally, e-mail can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an e-mail in relation to their age and good network etiquette; 'netiquette'.

The Google Hub is an integrated set of interactive online services that provide teachers, pupils and parents with information, tools and resources to support and enhance educational delivery and management. The school shows the children how to responsibly interact with one another via the Hub – showing respect, collaborating and communicating with each other. In the context of school, e-mail and the Hub should not be considered private.

- The school gives all staff their own e-mail account to use for all school business as a work based tool. This is to minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed. Under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses.
- It is the responsibility of each account holder to keep the password to both their email and learning platform accounts secure.
- For the safety and security of users and recipients, all mail is filtered and logged; if necessary e- mail histories can be traced. The school email account should be the account that is used for all school business.
- Children are taught how to successfully and safely use email and each child will be given their own personal Cleves School email address. Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.
- All pupil e-mail users are expected to adhere to the generally accepted rules of netiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments.
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail.
- Staff must inform the ICT coordinator or Deputy Headteacher if they receive an offensive e-mail.
- The forwarding of chain letters is not permitted.
- However the school e-mail is accessed, (whether directly, through webmail when away from the office or on non-school hardware), all the school e-mail policies apply.
- Pupils must not arrange to meet any person that they have only ever previously met on the Internet or by email or in a chat room, unless a parent, guardian or teacher has given them permission and they

take a responsible adult with them.
- Pupils must not place personal photos on any social network space provided in the school learning platform. Pupils will be advised to use nicknames and avatars when using social networking sites.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.

8. Pupils using mobile devices in the academy

Pupils may bring mobile devices into school, but are not permitted to use them during the school day unless permission is given by a member of staff.

9. Staff using work devices outside the academy

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed
- Mobile phones and associated cameras will not be used during lessons or formal school time except as part of an educational activity. The sending of abusive or inappropriate text messages is forbidden.
- Games machines including the iPod Touch, iPad and other handheld consoles (e.g. Nintendo DS) have Internet access which may not include filtering. Care will be taken with their use within the school.
- Staff will use a school phone where contact with pupils or parents is required. There may be a need to create messaging groups during school visits which allows Staff/Parent communication.

If staff have any concerns over the security of their device, they must seek advice from the SLT.

Work devices must be used solely for work activities.

10. How the academy will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our acceptable use policy. Complaints of Internet misuse will be dealt with by a senior member of staff. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures and staff code of conduct. Any complaint about staff misuse must be referred to the appropriate line manager. Complaints of a child protection nature must be dealt with in accordance with Cleves school child protection procedures. Pupils and parents will be informed of consequences for pupils misusing the Internet. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident. A breach or suspected breach of policy by a School employee, contractor or pupil may result in the temporary or permanent withdrawal of School ICT hardware, software or services from the offending individual.

The academy will consider whether incidents which involve illegal activity or content, or otherwise serious incidents should be reported to the police. Any policy breach is grounds for disciplinary action in accordance with the School Disciplinary Procedure. Policy breaches may also lead to criminal or civil proceedings.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL (and deputies) will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Trustees will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.