

<b>Policy</b>	<b>The Safe Use of Online Technology</b>
<b>Issue Date</b>	<b>1<sup>st</sup> September 2023</b>
<b>Review Date</b>	<b>1<sup>st</sup> September 2024</b>
<b>Author/s</b>	<b>Lucy Deakin &amp; Ashleigh Duncan</b>

### **Croyland Primary School: The Safe Use of Online Technology**

*This document details how we ensure the safe use of online technologies at Croyland Primary School. It is shared with staff as part of their employment induction and there on annually as part of the September Child protection and Safeguarding updates.*

*Document audience: Governors, Teachers, Support Staff, Parents, Carers, Visitors to school*

This policy has been written using guidance and legislation recommended by Northamptonshire Local Authority. Due to the ever-changing nature of online technologies, this policy is reviewed and updated annually.

#### **Policy Purpose:**

At Croyland Primary School, we recognise that keeping children safe when using technology is a necessary part of our safeguarding strategy. From experience, even with teaching, when caught in the “online world”, many children do not apply the learning that they articulate so well in the classroom setting.

Teaching our pupils how to keep safe in the “online world” and how to behave in a manner that is not detrimental to the wellbeing of others is a persistent and very real worry for us here at Croyland.

In addition, staff need to know what is expected of them with regard to their conduct in the “online world”. A lack of clarity could make individuals professionally vulnerable.

The purpose of this policy is to make clear to all, regardless of their role, the school safeguarding expectations in the use of “online technologies”. As a collective, we can then keep ourselves and our children safe and enjoy the advantages that technology can bring to our lives.

#### **Scope of Policy:**

This policy applies to the audience stated above who access the internet on a school device, or use their own device on our school premises. This policy is also applicable where school staff or individuals have been provided with school issued devices for use off-site, such as a school laptop or work mobile phone.

This policy document is organised into four parts

- **Part 1 - The roles and responsibilities expected of all school staff:**
- **Part 2 - Teaching our school community to keep safe:**
- **Part 3 – The safe use of school and personal ICT equipment:**
- **Part 4 - In the event of technology misuse:**
- **Appendix support:**

### ***Part 1 - The Roles and Responsibilities expected of all school staff:***

As a school community we expect all individuals to model safe online practices and lead by personal example.

All individuals visiting the school site and using a device to support their visit must read and follow the guidance in the relevant Acceptable Use Agreement.

The potential use of a device will be ascertained when the visitor or contractor signs into the school office. The relevant documentation will then be shared.

#### ***Headteacher and Governors:***

The Headteacher (DHT) and Governors have overall responsibility for online safety as part of the wider remit of Child protection and safeguarding. To ensure these responsibilities, the Head teacher and Deputy Headteacher, on behalf of the Governing Body will:

- Designate an Online Safety Lead - Ashleigh Duncan - to implement procedures, school staff training, review and amend curriculum requirements and take the lead responsibility for ensuring online safety is taught to all pupils.
- Ensure a safe, secure and appropriately filtered internet connection for school staff and pupils within the school. (Delegated to Martin Sewell).
- Provide resources and time for the online safety lead and employees to be trained and update written procedures where appropriate.
- Promote online safety across the curriculum and have a robust understanding of the impact of this teaching. (Delegated to Ashleigh Duncan)
- Ensure that any equipment which holds sensitive or confidential information and leaves school premises (e.g. iPads, school staff laptops and memory sticks) is encrypted (Delegated to Martin Sewell).
- Share any online safety and curriculum updates at Governing Body meetings and ensure that all present understand the link to child protection.
- Ensure that online safety is embedded within all safeguarding and child protection training, guidance and practices.

- Elect an Online safety Governor to ensure that all roles and responsibilities are being actioned.

### ***Online Safety Leader:***

The nominated Online Safety Lead must be an advocate for online safety and is the lead individual within our school for ensuring safe online practices are understood and actioned by all. They are also the individual who ensures our children and their families understand the potential dangers that are relevant to them through reviewing and amending our curriculum provision, sharing guidance and publications within newsletters and on our website as well as, speaking to and supporting families directly as situations occur.

Our nominated lead is Ashleigh Duncan. Her role includes:

- Communicating the importance of online safety and, our duty of care for the safety of our pupils and staff. Making clear to all, the potential for serious child protection / safeguarding issues to arise from: sharing of personal data; access to illegal / inappropriate materials; inappropriate online contact with adults / strangers; potential or actual incidents of grooming; online-bullying
- With the support of the ICT Technician, ensuring that filtering is set to the correct level for employees and pupils accessing school equipment.
- Strategically reporting areas of concern to the DSL and DDSLs through the wider safeguarding agenda which is reported to the governing body.
- Liaising with key members of school staff to ensure that any emerging online safety issues are addressed and actioned appropriately
- Co-ordinating and delivering employee training according to new and emerging technologies so that the correct online safety information is being delivered.
- With the support of the ICT Technician, implementing a system of monitoring employee and pupil use of school issued technologies and the internet where appropriate. This will be in the form of random spot-checks which will be completed on a monthly basis and reported to the online safety lead.
- Monitor the contact of EYFS Facebook account to ensure the team do not post anything that can be considered as a breach of copyright, data protection or any other legislation.
- Undertaking training in current and emerging online safety issues.
- Listening to and using the information provided by our pupils to ensure we are tuned into their world.
- Reviewing and monitoring curriculum entitlement annually.
- Providing online safety advice and updates on risks and risk management through the school newsletter and school website.

- Facilitating online support for parents to provide continued awareness of the benefits and potential risks related to technologies and their role in which to manage these.

### ***ICT Technician:***

***Our appointed ICT technician is Martin Sewell.***

The role of the ICT technician is to ensure the school network is secure and not open to misuse or malicious attack compromising the online safety of our school staff and pupils. The list below encompasses the core aspects of their role with regard to online safety. This is not an exhaustive list of their whole role. Their role includes ensuring that:

- Anti-virus software is installed and maintained on all school machines and portable devices.
- The school's filtering policy is applied and updated on a regular basis and that responsibility for its implementation is shared with the Online Safety Lead and the DSL.
- Any problems or faults relating to filtering are reported to the DSL and to the broadband provider immediately and recorded on an Online Safety Incident Log.
- Users may only access the school's network through a registered account created on the active directory; requiring a password to logon.
- All pupil users at Year 2 and above will be provided with a username and secure password by the ICT technician who will keep an up to date record of users and their usernames.
- They maintain an up to date technical knowledge in order to maintain the security of the school network and safeguard children.
- They regularly monitor the school's network in order that any deliberate or accidental misuse can be reported to the Online Safety Lead or DSL.
- Servers, wireless systems and cabling are securely located and physical access restricted.
- Administrator passwords for the school ICT systems, used by the Network Manager, are made available to the Headteacher or other nominated senior leader and kept in a secure place.
- All users have clearly defined access rights to school systems.

### ***Teaching Staff – including Teacher Assistants:***

All teachers and teacher assistants have a responsibility to ensure that their pupils access online technologies appropriately and safely.

All teaching school staff, as defined above, are provided with annual training and continuous updates via the online safety lead.

They are responsible for:

- Teaching online safety in line with the recommended curriculum and, embedding these lessons throughout the curriculum and discussing them as and when relevant.
- Making explicit the requirements of the acceptable use agreement and model the expectations in use of all online technology.
- Reporting any suspected filter breaches, misuse or pupil online safety concerns to the *Online Safety Lead, or DSL in their absence*, for investigation.
- Monitoring the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and ensure school expectations are maintained with regard to these devices
- Ensuring that pre-planned use of online material is checked to ensure that it is suitable and appropriate.

### ***Our pupils:***

How to use online technologies safely is embedded into our IT curriculum and day to day school life as required in individual circumstances.

Within our curriculum provision, our pupils are taught what acceptable use is and the potential dangers that come with accessing online technologies. In doing so, and by revisiting often, we hope our pupils will:

- Inform school staff of any inappropriate materials, cyberbullying or contact from unknown sources (age dependant).
- Inform teaching school staff of online situations which impact on their wellbeing.

In her role, our online safety leads talks to our pupils within cohort groups, in order to understand their worries, to hear their experiences and to ensure we remain in tune with their worlds and our teaching and guidance is current.

### ***Part 2 - Teaching our school community how to keep safe:***

#### ***School staff:***

Formal online safety training takes place upon a new employee's induction to the school and, annually alongside the review of our Child Protection and Safeguarding training. In addition to this, regular updates are shared in the school staff bulletin and email as and when required.

## Parent/Carer involvement:

As part of the school's commitment to developing online safety awareness amongst children and young people, every effort is made to engage parents and carers in the process.

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 online behaviours.




In our experience, many parents and carers underestimate how often children and young people come across potentially harmful and inappropriate material on the internet or do not take in account age ratings (PEGI Ratings). They are often unsure how to set filters and controls. To support parents and carers, we provide information and awareness through:

- Curriculum activities;
- Letters, newsletters, website;
- Support from the school ICT technician where required;
- Parents / Carers evenings;
- High profile events e.g. Safer Internet Day
- Reference to the relevant web sites / publications e.g. [swgfl.org.uk](http://swgfl.org.uk)  
[www.saferinternet.org.uk/](http://www.saferinternet.org.uk/) <http://www.childnet.com/parents-and-carers>
- On their first time entry to the school, and on entry to key stage 2, pupils and their parents/carers are both asked to read and sign acceptance of the rules, a copy of which will be given to parents and carers to reference at home.




## Our pupils:

Through the curriculum our pupils will be taught to both recognise and manage the risks presented from the 3C's being:



### Conduct

-  Children need to be aware of the impact that their online activity can have on both themselves and other people, and the digital footprint that they create on the internet.
-  It's easy to feel anonymous online and it's important that children are aware of who is able to view, and potentially share, the information that they may have posted.
-  When using the internet, it's important to keep personal information safe and not share it with strangers.

### Content

-  Some online content is not suitable for children and may be hurtful or harmful. This is true for content accessed and viewed via social networks, online games, blogs and websites.
-  It's important for children to consider the reliability of online material and be aware that it might not be true or written with a bias.
-  There can be legal consequences for using or downloading copyrighted content, without seeking the author's permission.

### Contact

-  It is important for children to realise that new friends made online may not be who they say they are and that once a friend is added to an online account, you may be sharing your personal information with them.
-  If you have concerns that a pupil is, or has been, the subject of inappropriate sexual contact or approach by another person (including, but not limited to, a request to meet up or a request for images/videos), it's vital that you report it to your Designated Safeguarding Lead who can liaise with the police via the Child Exploitation and Online Protection Centre ([www.coop.police.uk](http://www.coop.police.uk)).

The school follows the Project Evolve curriculum which empowers learners to think critically, behave safely and participate responsibly in online activity. It promotes digital resilience; focusing on developing strategies to identify and manage risks rather than the removing of technologies.

Teachers are expected to adapt sessions for any child with special educational needs to ensure that all pupils are able to access online provision at an appropriate level.

Pupils are made aware of the importance of managing their online image and relationships, cyberbullying, copyright issues, data protection, intellectual property, reporting concerns and reliability of information sourced on the internet as part of the online safety curriculum.

Safer Internet Day is celebrated annually to raise the profile of online safety amongst school staff and pupils.

### ***PART 3 - Use of School and Personal ICT Equipment:***

***If following reading part 3 of this policy document, you are unsure in any way of the expectations placed upon you, please do not hesitate in speaking to the IT lead.***

#### ***Emails:***

##### ***School staff (Including Governors):***

- The school provides all school staff and governors with a professional email account to use for all school related business. This allows for email content to be monitored and protects school staff from the risk of allegations, malicious emails or inappropriate contact with children and their families.
- Under no circumstances **must any member of school staff** engage in any personal communications (i.e. via personal email, Whatsapp or social media accounts) with current or former pupils outside of authorised school systems. (Family members excluded)
- School staff should inform the ICT Technician or the Online Safety Lead if they receive an offensive or inappropriate email via the school system.
- School staff are advised that if they use a mobile phone or tablet to access their emails, that they do this using the web browser rather than an email application, which is often accessible without a password.

It is the responsibility of each account holder to keep their password secure and to report any suspected breaches of password security to the Online Safety Lead, ICT Technician or class teacher

Account holders must never share their password with another user, or allow access to their email account without the express permission of the Headteacher.

### ***Laptops/iPads:***

- School staff must ensure that all sensitive school data is stored on the network (shared drive) and not solely on the laptop or device, unless the device is encrypted. In the event of loss or theft, failure to safeguard sensitive data could result in a serious security breach and subsequent fine. Password protection to your device alone is not sufficient.
- School staff are provided with laptops to allow for school related work to be completed off site. Personal use of the laptop from home (such as web browsing/online shopping etc) is permitted but should be kept to a minimum and use of the device is strictly restricted to the authorised member of school staff only (i.e. not family members)
- School staff are aware that all activities carried out on school devices and systems, both within and outside of the school environment, will be monitored in accordance with this policy.
- School staff must ensure that school laptops and devices are made available as necessary for anti-virus updates, software installations, patches, upgrades or routine monitoring/servicing.
- It is made clear to all school staff that if they ignore Acceptable Use procedures, security advice or use email or the internet for inappropriate reasons, they risk dismissal and possible police involvement.

### ***Removable Media (Memory Sticks/USB):***

- Where school staff require removable media to store or access sensitive data (e.g. ASPs, pupil attainment and assessment data) off site, only encrypted memory sticks must be used. These are made available to all teachers and to those school staff who require them because they work directly with children.
- Any passwords used for encrypted memory sticks/or other devices will be remain confidential to the user and shared only with authorised IT personnel for security and monitoring purposes.

### ***Mobile Phones:***

- All staff should ensure that their mobile telephones are left on silent and kept with their personal belongings, out of the sight of children
- If a staff member requires their mobile phone to be on, due to a significant personal circumstance (e.g. acutely sick relative), this must be approved by a member of the Senior Leadership Team.
- Permission will only be granted for exceptional reasons; it is the responsibility of the member of staff to inform the staff and pupils they are working with. The



Governing Body insists that in giving this permission, the member of staff acts as a role model of good mobile phone etiquette.

- In addition, they request that the member of staff make it very clear to the pupils they are working with, that during work time/learning time, mobile phone communication is not generally allowed.
- If a phone call is received, the call must not be continued in depth until the member of staff is in a private place away from all children and supervision has been made for the children.
- Making and receiving personal calls/text messages can be made during break/lunch times, not during teaching time or in any area that is public to children and their parents. This includes outdoor spaces which are accessible to children, e.g. outside reception.
- Calls can be made from a classroom but no children must be present and measures must have been taken to prevent children entering your space.
- If the above expectations are not followed, a warning may be given to the member of staff and this will be held on their personnel file.
- Where a member of staff has been named as an emergency contact, or next of kin, the school office number must be given as first priority, rather than a personal number. The school office staff will ensure that the staff member is immediately informed of such phone calls and will ensure that a private space is made available to take the call.
- School staff are not at any time permitted to use photographic or recording equipment on their mobile phone, for example: to take recordings of children, or sharing images. Legitimate recordings/photographs should be captured using school equipment e.g. cameras/iPad.
- School staff should report any mobile phone use that breaches the expectations above or, that causes them concern, to a member of the senior leadership team.
- The Headteacher, or Deputy Headteacher in her absence, reserves the right to check the image contents of a member of school staff's mobile phone or mobile devices should there be any cause for concern over the inappropriate use of it. Should inappropriate material be found then the Local Authority will be contacted immediately for advice.

### ***Mobile Phones for work related purposes:***

We recognise that mobile phones provide a useful means of communication on offsite activities. However, school staff should ensure that:

- Mobile phone use on these occasions is appropriate and professional (and will never include taking photographs of children).
- Every effort should be made to ensure that any parental telephone contact is made through the school mobile phone. However, if this is not possible and a personal mobile phone is used, the caller's number must be withheld and the contact number must then be deleted after the call. No text messages should be

sent from school staff member's personal mobile phone to a parent about a school related issue. Our text service, teachers2parents, serves this purpose.

- Where parents are accompanying their children on trip, they are informed by the visit leader that they must not make contact with other parents (via calls, text, email or social networking) during the trip or use their mobile phone to take photographs of children.

### ***Expectation of Parental mobile phone use on site:***

While we would prefer parents not to use their mobile phones while at school, we recognise that this would be impossible to regulate and that many parents see their phones as essential means of communication at all times. We continually ask that parents' usage of mobile phones, whilst on the school site, is courteous and appropriate to the school environment.

We allow parents to photograph or video school events such as shows or sports day using their mobile phones, but insist that parents do not publish images (e.g. on social networking sites) that include any children other than their own.

If it becomes apparent that this request has been breached, the parent or family member concerned will be asked to remove them from public view.

### ***Social Networking:***

Regardless of the role of the staff member, personal social networking sites must not be used within school hours on any device unless on an allocated break and in a designated space where children are not permitted to enter.

It is made clear that their behaviour in their personal lives may impact upon their reputation and continued employment in our school if for some reason, out of school behaviour becomes public and is deemed a safeguarding concern, an illegal act or puts the reputation of the school into disrepute.

School staff are informed that network activity and online communications on school equipment (both within and outside of the school environment) may be monitored, including any personal use of the school network as part of our safeguarding procedures.

School staff are also reminded to

- set privacy settings to minimise the opportunity of being contacted by school community members
- seek advice from the Headteacher if contacted by a current/ previous pupil under the age of 18 via social media

- seek advice if another school staff member has posted a picture/video on personal social media of children in the school.
- not post a comment, picture or video that could upset anyone in the school community
- not post anything online that they would not ordinarily share with the Headteacher.

### ***Appropriate use of the school social networking account***

Please refer to the appendices for guidance regarding the use of the school social networking sites to support parental engagement.

### ***Photographs and Videos:***

Digital photographs and videos are an important part of the learning experience for children and, as such, schools have a responsibility to ensure that they not only educate pupils about the safe and appropriate use of digital imagery, but also model good practice themselves. At our school:

- Written consent will be obtained from parents or carers before photographs or videos of their children will be taken or used within the school environment, including the school website or associated marketing material.
- Permission will be sought from a pupil or school staff member before an image or video is taken and the purpose of the activity and intended use of the image will be made clear. If it is to be shared within the school community, the individual must be asked beforehand.
- School staff are not permitted to use personal devices, such as cameras, video equipment or camera phones, to take photographs or videos of pupils. However, in exceptional circumstances, such as equipment shortages, permission may be granted by the Headteacher for use of personal equipment for school related photographs or videos, provided that there is an agreed timescale for transfer and deletion of the image from the school staff member's device.
- Photographs of pupils must not be published or displayed on the school website.

### **Visiting Teachers: (NMPAT)**

When our visiting teachers wish to make recordings of their pupils performing, this must be **made as an audio file unless a school device is requested**. This is also the expectation from NMPAT. A request for a school device must be made to Mrs Beavis who will share the photograph or film with the parent/carer of the child.

## ***Video Conferencing:***

We continue to use Zoom within the school for whole school assemblies. To promote safety, all sessions will be password protected and participants will need an invitation to attend. These details will be emailed to prior to the event to the class teacher. A member of the teaching staff will be present in each classroom throughout the whole zoom meeting.

## ***PART 4 - In the event of technology misuse:***

Online Safety is an ever growing area and is always developing as things are constantly changing it is extremely difficult to safeguard against every situation. At Croyland Primary School, we aim to ensure that our children are always kept safe when using technologies, however we cannot guarantee a complete safeguard. School staff are trained in how to manage the situation should a child be exposed to inappropriate material.

In the event of technology misuse by a member of school staff or pupils, including use of the school network in an illegal, unsuitable or abusive manner, a report must be made to the Headteacher/ Deputy Headteacher and the lead teacher for online safety immediately.

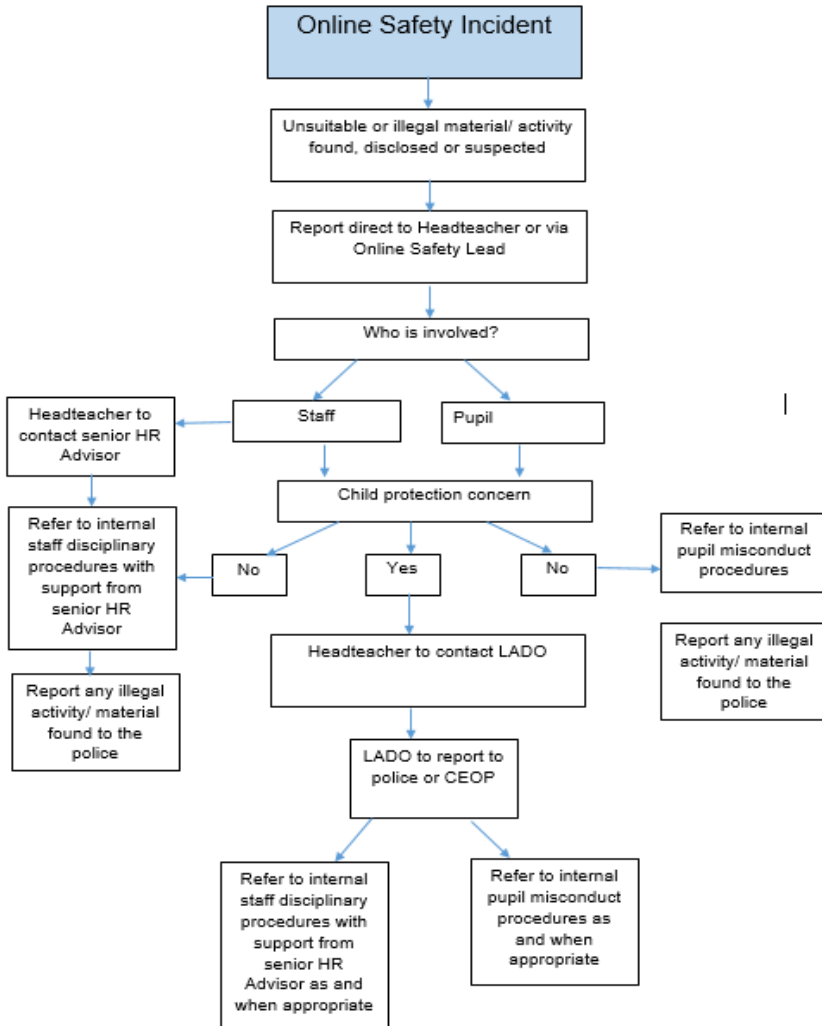
In the event of minor or accidental misuse, internal investigations should be initiated and disciplinary procedures followed where appropriate. Additionally, all security breaches, lost/stolen equipment or data, unauthorised use or suspected misuse of ICT must be reported immediately to the Headteacher, ICT Technician School Business Manager.

Any concerns about a child in regard to an online safety issue, should be recorded on MyConcern and tasked to the Online Safety Lead to be actioned. If this is not possible, then it should be written down on an Online Safety CAR log for the Online Safety Lead to add to MyConcern and address.

An overview of all incidents is compiled into a report termly, which is shared at a wider safeguarding meeting. This report summarises all completed actions and any subsequent provision required to improve school staff, pupil and parent awareness.

In order to prevent possible misuse of technology by school staff, all members of school staff are requested to read this policy annually and sign confirmation of this.

Where a member of school staff is in breach of this policy they may be subject to investigation by the school, local authority, and/or the police. This may result in a disciplinary, a dismissal, or legal action being taken against them. In the event of any of the above, HR guidance will be requested. See flow chart below.



## Appendix Support:

### Appendix 1 Croyland Primary School Network Systems and Security

#### **Monitoring Usage**

- The web filter provided by *Netsweeper* monitors school staff usage, and flags up any inappropriate use to the ICT Web Technician. This is reviewed monthly, and any concerns are reported straight to the Headteacher.
- The ICT Web Technician regularly monitors and record user activity, including any personal use of the school ICT system (both within and outside of the school environment). School staff are made aware of this.
- Each month, the ICT Web Technician remotely checks 3 school staff laptops to check that content which is accessed at home is of an appropriate nature. This information is shared with the Designated Senior People.
- The ICT Web Technician is checked at random by the governor who monitors Online Safety. At present, this is Sean Roberts.

#### **Internet Access and Age Appropriate Filtering**

Broadband Provider: Talk Straight

All pupils are entitled to safe and secure internet access and schools have a duty to deliver this as part of the learning experience. The Head teacher is ultimately responsible for ensuring that the school infrastructure and network is as safe and secure as is reasonably possible and that age appropriate internet filtering is in place to protect young users from inappropriate or harmful online content. To this end, the school has the following filtering measures in place:

- Filtering levels are managed and monitored in school via an administration tool/control panel, provided by our broadband supplier, which allows our ICT Web Technician to instantly allow or block access to a site or specific pages and manage user internet access.
- Filtering levels are managed and monitored on behalf of the school by our broadband supplier or technical support, allowing an authorised school staff member to allow or block access to site and manage user internet access.
- Age appropriate content filtering is in place across the school, ensuring that school staff and pupils receive different levels of filtered internet access in line with user requirements (e.g. YouTube at school staff level but blocked to pupils)
- All users have unique usernames and passwords to access the school network which ensures that they receive the appropriate level of filtering. Class log-ins, dependent on age, may also be used.

In addition to the above, the following safeguards are also in place:

- Anti-virus and anti-spyware software is used on all network and standalone PCs or laptops and is updated on a regular basis.
- A firewall ensures that information about children and young people cannot be accessed by unauthorised users.
- Encryption codes on wireless systems prevent hacking
- The CEOP Report Abuse button is available on the school website to allow pupils or school staff to report online safeguarding issues.
- We use a secure version of *Google* as our search engine as an additional safeguard.