FOXHILLS FEDERATION ONLINE SAFETY POLICY

Status	Current	**Approval**	Full Governing Body
Review frequency	2 Years	**Author (role)**	Lucy Howe
Date effective	November 2023	**Date approved**	27th November 2023
Date of next review	October 2025	**Date withdrawn**	N/A

Core Principles of the E-Safety Policy

Pupils, across both our schools, are growing up in an increasingly complex world, living their lives seamlessly on and offline. This presents many positive and exciting opportunities, but also challenges and risks. We aim to equip our pupils with the knowledge needed to make the best use of the internet and technology in a safe, considered and respectful way, so they are able to reap the benefits of the online world.

We achieve this by:

Curriculum context

Through our relationships and PSHE curriculum, pupils are taught about online safety and harms. These are known as the 4Cs- commerce, conduct, content, contact. Teaching the 4Cs includes:

- What constitutes positive, healthy and respectful online relationships
- the effects of their online actions on others
- how to recognise and display respectful behaviour online

During teaching, teachers will address online safety and appropriate behaviour in an age-appropriate way that is relevant to our pupil's lives. This complements our computing curriculum, which covers the principles of online safety at all key stages, with progression in knowledge and content to reflect the different and escalating risks that pupils face. This includes:

- how to use technology safely, responsibly, respectfully and securely
- where to go for help and support when they have concerns about content or contact on the internet or other online technologies

PSHE, pupil voice and the teaching of fundamental British values, include content relevant to teaching pupils how to use the internet safely. For example:

- freedom of speech
- the role and responsibility of the media in informing and shaping public opinion
- the concept of democracy, freedom, rights, and responsibilities

Teaching underpinning knowledge and behaviour

The online world develops and changes at a great speed. New opportunities, challenges and risks are appearing all the time. To ensure both schools stay up to date with the with the latest devices, platforms, apps, trends and related threats, we focus on the underpinning knowledge and behaviours that can help pupils to navigate the online world safely and confidently, regardless of the device, platform or app they are using. We achieve this by:

- building this into existing lessons across the curriculum
- specific online safety lessons
- school-wide approaches- acceptable use agreements, IT protocol, assemblies, website information for our families.

Evaluating what our pupils see online

We enable our pupils to make judgements about what they see online and to not automatically assume that what they see is true, valid or acceptable.

Our teaching, across a range of subjects, focuses on:

- whether a website, URL or email is fake
- what cookies do and what information they are sharing
- if a person or organisation is who they say they are

- why a person wants them to see, send or believe something
- why a person wants their personal information
- the reason why something has been posted
- whether something they see online is fact or opinion

Recognising techniques used for persuasion

We teach our pupils to recognise the techniques that are often used to persuade or manipulate others:

- online content which tries to make people believe something false is true or mislead (misinformation and disinformation)
- techniques that companies use to persuade people to buy something
- ways in which criminals may try to defraud people online
- ways in which games and social media companies try to keep users online longer (persuasive or sticky design)
- grooming and manipulation techniques used by criminals
- ways to protect themselves from a range of cyber crimes

Online behaviour

Our pupils must understand what acceptable and unacceptable online behaviour look like. We teach the children:

- that the same standard of behaviour and honesty apply on and offline, including the importance of respect for others
- to recognise unacceptable behaviour in others

We help pupils to recognise acceptable and unacceptable behaviour by:

- looking at why people behave differently online, for example how anonymity (you do not know me) and invisibility (you cannot see me) affect what people do
- looking at how online emotions can be intensified resulting in mob mentality
- looking at the key principles behind a constructive discussion, including a willingness to listen to other opinions and a readiness to be educated on a topic
- considering how to demonstrate empathy towards others (on and offline)
- teaching techniques (relevant on and offline) to defuse or calm arguments, for example, a disagreement with friends, and disengage from unwanted contact or content online
- considering unacceptable online behaviours often passed off as so-called social norms or just banter, for example, negative language being used as part of online gaming but would never be tolerated offline

Identifying online risks

We support our pupils to identify possible online risks and make informed decisions about how to act. Our teaching educates children to assess situations, to think through the consequences of acting in different ways and to decide on the best course of action.

We do this by discussing:

- the ways in which someone may put themselves at risk online
- risks posed by another person's online behaviour
- when risk taking can be positive and negative
- online reputation and the positive and negative aspects of an online digital footprint
- sharing information online and how to make a judgement about when and how to share and who to share with
- the risks of cyber- crime, online fraud and identity theft

How and when to seek support

Our pupils must know the safe ways in which to seek support if they are concerned or upset by something they have seen online.

Our pupils and their parents know how to:

- identify who trusted adults are
- access support from the school, police, the National Crime Agency's Click CEOP reporting service for children and 3rd sector organisations such as Childline and Internet Watch Foundation

- report cyber crime, fraud and suspicious online activity, through organisations such as Action Fraud and the Advertising Standards Authority
- report inappropriate contact or content for various platforms and apps

Online media literacy strategy

Both schools have regard for the online media literacy strategy and use the strategy to provide our pupils, as internet users, with the knowledge and skills they need to make informed and safe choices online.

The five principles feature as part of our computing, safeguarding and PSHE curriculum:

- the risks of sharing personal data and how to protect their privacy
- how the online environment operates
- how online content is generated and to critically analyse the content they consume
- that online actions can have offline consequences, and use this understanding in their online interactions
- how to participate positively in online engagement, while understanding the risks of engaging with others

Teaching about harms and risks

Understanding and applying knowledge and behaviours will provide our pupils with a solid foundation to navigate the online world in an effective and safe way. By understanding the risks that exist online, we have tailored our teaching and guidance to the specific needs of our pupils, which include:

How to navigate the internet and manage information

The technical aspects of the internet that could leave pupils vulnerable if not understood. Our E-safety website page provides age-specific advice on these potential harms and risks:

- managing online information
- copyright and ownership
- privacy and security

Age restrictions

Some online activities have age restrictions because they include content which is not appropriate for children under a specific age. Our teaching and advice includes:

- explaining that age verification exists and why some sites require a user to verify their age, for example, online gambling and purchasing of certain age restricted materials such as alcohol
- explaining why age restrictions exist, for example, they provide a warning that the site may contain disturbing material that is unsuitable for younger viewers
- helping pupils understand how this content can be damaging to under-age consumers
- explaining what the age of digital consent means - the minimum age (13) at which young people can agree to share information and sign up to social media without parental consent under General Data Protection Regulations

How content can be used and shared

Knowing what happens to information, comments or images that are put online enables our pupils to understand about digital footprints. Our teaching includes:

- what a digital footprint is, how it develops and how it can affect future prospects such as university and job applications
- how cookies work
- how content can be shared, tagged and traced
- how difficult it is to remove something a user wishes they had not shared
- the risk of identity theft or targeted approach from fraudsters using information shared online
- ensuring pupils understand what is illegal online, for example:
    - youth-produced sexual imagery (sexting)
    - sharing illegal content such as extreme pornography or terrorist content
    - the illegality of possession, creating or sharing any explicit images of a child even if created by a child

Disinformation, misinformation, malinformation and hoaxes

Some information shared online is accidentally or intentionally wrong, misleading, or exaggerated. We help our pupils to understand this by teaching:

- disinformation and why individuals or groups choose to share false information in order to deliberately deceive

- misinformation and being aware that false and misleading information can be shared inadvertently
- malinformation and understanding that some genuine information can be published with the deliberate intent to harm, for example releasing private information or photographs (including revenge porn)
- online hoaxes, which can be deliberately and inadvertently spread for a variety of reasons
- explaining that the viral nature of this sort of content can often appear to be a stamp of authenticity and therefore why it is important to evaluate what is seen online
- how to measure and check authenticity online
- the potential consequences of sharing information that may not be true

Fake websites and scam emails
Fake websites and scam emails are used to extort data, money, images and other things that can either be used by the scammer to harm the person targeted or sold on for financial, or another gain. Our pupils are taught:

- how to look out for fake URLs and websites
- ensuring pupils understand what secure markings on websites are and how to assess the sources of emails
- explaining the risks of entering information to a website which isn't secure
- what to do if harmed, targeted or groomed as a result of interacting with a fake website or scam email
- who to go to and the range of support that is available
- explaining the risk of 'too good to be true' online offers, advertising and fake product sales designed to persuade people to part with money for products and services that do not exist

Fraud (online)
Fraud can take place online and can have serious consequences for individuals and organisations. We teach:

- what identity fraud, scams and phishing are
- explaining that online fraud can be highly sophisticated and that anyone can be a victim
- how to protect yourself and others against different types of online fraud
- how to identify 'money mule' schemes and recruiters
- the risk of online social engineering to facilitate authorised push payment fraud, where a victim is tricked into sending a payment to the criminal
- the risk of sharing personal information that could be used by fraudsters
- explaining that children are sometimes targeted to access adults' data, for example, passing on their parent or carer's bank details, date of birth or national insurance number
- what good companies will and won't do when it comes to personal details, for example, a bank will never ask you to share a password or move money into a new account
- how to report fraud, phishing attempts, suspicious websites and adverts

Password phishing
Password phishing is the process by which people try to find out your passwords so they can access protected content. We teach:

- why passwords are important, how to keep them safe and that others may try to trick you to reveal them
- explaining how to recognise phishing scams, for example, those that try to get login credentials and passwords
- the importance of online security to protect against viruses (such as keylogging) that are designed to access, steal or copy passwords
- what to do when a password is compromised or thought to be compromised

Personal data
Online platforms and search engines gather personal data. This is often referred to as 'harvesting' or 'farming', and we teach our pupils:

- how cookies work
- how data is farmed from sources which look neutral, for example, websites that look like games or surveys that can gather lots of data about individuals
- how, and why, personal data is shared by online companies, for example, data being resold for targeted marketing by email and text (spam)
- how pupils can protect themselves, including what to do if something goes wrong (for example data being hacked) and that acting quickly is essential
- the rights children have with regard to their data, including particular protections for children under the General Data Protection Regulations (GDPR)
- how to limit the data companies can gather, including paying particular attention to boxes they tick when playing a game or accessing an app for the first time

Persuasive design
Many devices, apps and games are designed to keep users online for longer than they might have planned or desired. We help our pupils to understand:

- that the majority of games and platforms are businesses designed to make money - their primary driver is to encourage users to be online for as long as possible to encourage them to spend money (sometimes by offering incentives and offers) or generate advertising revenue
- how designers use notifications to pull users back online

Privacy settings
Almost all devices, websites, apps and other online services come with privacy setting that can be used to control what is shared. We support our pupils and Parents to:

- find information about privacy setting on various sites, apps, devices and platforms
- explaining that privacy settings have limitations, for example, they will not prevent someone posting something inappropriate

Targeting of online content (including on social media and search engines)
Much of the information seen online is a result of some form of targeting. As such, we teach:

- how adverts seen at the top of online searches and social media feeds have often come from companies paying to be on there and different people will see different adverts
- how the targeting is done, for example, software which monitors online behaviour (sites they have visited in the past, people who they are friends with) to target adverts thought to be relevant to the individual user
- the concept of clickbait and how companies can use it to draw people onto their sites and services

We cover all of the above content through:

- relationships education
- health education
- computing
- citizenship in KS2

<u>Teaching our pupils to stay safe online</u>
Abuse (online)
Some online behaviours are abusive. They are negative in nature, potentially harmful and in some cases can be illegal. Our teaching focuses on:

- explaining about the types of online abuse including sexual, harassment, bullying, trolling and intimidation
- explaining when online abuse can cross a line and become illegal, such as forms of hate crime and blackmail
- how to respond to online abuse including how to access help and support
- how to respond when the abuse is anonymous
- discussing the potential implications of online abuse, including the implications for victims
- being clear about what good online behaviours do and don't look like

Online radicalisation
Children, young people and adult learners are at risk of accessing inappropriate and harmful extremist content online. This could include downloading or sharing terrorist material, which could be a criminal act. We understand that the internet and social media make spreading divisive and hateful narratives easier. Extremist and terrorist groups and organisations use social media (for example, apps, forums, blogs, chat rooms) to identify and target vulnerable individuals. We teach our pupils:

- how to recognise extremist behaviour and content online
- understanding actions which could be identified as criminal activity
- exploring techniques used for persuasion
- knowing how to access support from trusted individuals and organisations

Under the Prevent duty, we build our pupil's resilience to extremism and ensure staff are adequately trained to spot the signs of radicalisation (annual training- see staff declarations).

Challenges
Online challenges acquire mass followings and encourage others to take part in what they suggest. We discourage our children from engaging with challenges because of the potential harm and risks they pose. We teach pupils:

- what an online challenge is and that while some will be fun and harmless, others may be dangerous and or even illegal
- how to assess if the challenge is safe or potentially harmful, including considering who has generated the challenge and why
- that it is ok to say no and not take part
- how and where to go for help if worried about a challenge
- the importance of telling an adult about challenges which include threat or secrecy ('chain letter' style challenges)

Content which incites
Knowing that violence can be incited online and escalate very quickly into offline violence. Our teaching includes:

- ensuring pupils know that online content (sometimes gang related) can glamorise the possession of weapons and drugs
- explaining that to intentionally encourage or assist an offence is also a criminal offence
- ensuring pupils know how and where to get help if worried about involvement in violence

Fake profiles
Not everyone online is who they say they are and it is important our pupils understand this. We teach:

- that in some cases profiles may be people posing as someone they are not (such as an adult posing as a child) or may be bots (which are automated software programs designed to create and control fake social media accounts)
- how to look out for fake profiles, for example:
    - profile pictures that don't like right, for example, of a celebrity or object
    - accounts with no followers or thousands of followers
    - a public figure who doesn't have a verified account

Grooming
We alert pupils and Parents to the different types of grooming and motivations for it, for example:

- radicalisation
- child sexual abuse and exploitation
- gangs (county lines)
- financial exploitation (money mules)

Our teaching includes:

- boundaries in friendships with peers, families and with others
- the key indicators of grooming behaviour
- explaining the importance of disengaging from contact with suspected grooming and telling a trusted adult
- how and where to report it both in school, for safeguarding and personal support, and to the police

At all stages, we balance teaching children about making sensible decisions to stay safe whilst being clear it is never the fault of a child who is abused and why victim blaming is always wrong.

Live streaming
Live streaming (showing a video of yourself in real-time online either privately or to a public audience) can be popular with children but it carries risk when carrying it out and watching it. Our curriculum teaches:

- the risks of carrying out live streaming such as the potential for people to record live streams without the user knowing and content being shared without the user's knowledge or consent
- that online behaviours should mirror offline behaviours and considering any live stream in that context - pupils shouldn't feel pressured to do something online that they wouldn't do offline
- the risk of watching videos that are being live streamed, for example, there is no way of knowing what will come next and so this poses a risk that a user could see something that has not been deemed age appropriate in advance
- explaining the risk of grooming

Unsafe communication
Knowing how to stay safe online when communicating with others, especially when it is with people they do not know or have never met, pupils must understand what constitutes safe contact: we teach:

- that communicating safely online and protecting your privacy and data is important regardless of who you are communicating with
- indicators or risk and unsafe communications
- risks associated with giving out addresses, phone numbers or email addresses to people you do not know or arranging to meet someone you have not met before
- about consent online and supporting pupils to develop strategies to confidently say "no" to both friends and strangers online

We cover all of the above content through:

- relationships education
- health education
- computing
- citizenship in KS2

Wellbeing

We recognise that certain elements of online activity can adversely affect a pupil's wellbeing:

- self-image and identity
- online reputation
- online bullying
- health, wellbeing and lifestyle

Impact on confidence (including body confidence)

It is important that our pupils know and understand about the impact of comparisons to 'unrealistic' online images. In KS2, we teach children about:

- the use of image filters and digital enhancement
- the role of social media influencers, including that they are paid to influence the behaviour (particularly shopping habits) of their followers
- that 'easy money' lifestyles and offers may be too good to be true
- looking at photo manipulation including discussions about why people do it and how to look out for it

Knowing how to identify when online behaviours stop being fun and begin to create anxiety, is reliant on pupils knowing that there needs to be a balance between time spent on and offline.

Teaching includes:

- helping pupils to evaluate critically what they are doing online, why they are doing it, and for how long (screen time)
- helping pupils to consider quality versus quantity of online activity
- explaining that pupils need to consider if they are actually enjoying being online or just doing it out of habit, due to peer pressure or the fear of missing out
- helping pupils to understand that time spent online gives users less time to do other activities - this can lead to some users becoming physically inactive
- exploring the impact that excessive social media usage can have on levels of anxiety, depression and other mental health issues
- explaining that isolation and loneliness can affect pupils and that it is very important for pupils to discuss their feeling with an adult and seek support
- where to get help

People can often behave differently online to how they would act face to face.

Our teaching includes:

- how and why people can often portray an exaggerated picture of their lives (especially online) and how that can lead to pressure
- discussing how and why people are unkind or hurtful online, when they would not necessarily be unkind to someone face to face

Reputational damage

We support our pupils to understand that what online users post can affect future career opportunities and relationships – both positively and negatively.

Teaching includes:

- looking at strategies for positive use
- how to build a professional online profile

Vulnerable pupils

Any pupil can be vulnerable online, and their vulnerability can fluctuate depending on their age, developmental stage and personal circumstance.

There are some pupils, for example, looked after children and those with special educational needs, who may be more susceptible to online harm or have less support from family or friends in staying safe online. With this mind, we consider all of our pupils individually and when vulnerabilities exist, we tailor our teaching and appropriately, to make sure our children receive the information and support they need.

Use of external visitors

Online safety can be a difficult and complex topic which changes very quickly. Therefore, as appropriate, we will seek external support from those who have expertise and up to date knowledge and information.

All external visitors are chosen with care and consideration, to ensure they can provide a useful and engaging approach to deliver online safety messages, by enhancing the school's offer (rather than be delivered in isolation). Our computing and PSHE curriculum mapping clearly plans for enrichment and wider personal development opportunities and all external support is sequentially planned with a clear rationale for "why this, why now".

Safeguarding

As with any safeguarding lessons or activities, it is important to consider the knowledge being taught and the potential that a child (or more than one child) in the class may be suffering from online abuse or harm in this way.

Consistent with our safeguarding principles and culture, it is important to create a safe environment where pupils feel comfortable to say what they feel- we would never wish for a child to feel they might get into trouble or be judged for talking about something which happened to them online.

When we are already aware of a child who is being abused or harmed online, we will carefully plan any lesson to consider this, including not drawing attention to that child in a way that would highlight or publicise the abuse. Consistent with policy, teachers will involve the designated safeguarding lead (or a deputy) when planning any safeguarding related lessons or activities (including online) as they will be best placed to advise on any known safeguarding cases, and how to support any pupils who may be especially impacted by a lesson.

In some cases, following a lesson or activity, some pupils may wish to disclose- the lesson may have provided the knowledge that enables the child to realise they are being abused or harmed or give them the confidence to say something. This is why it is essential all pupils are clear what the school's reporting mechanisms are (we listen to children, children can share anything with adults but this information is usually shared with DSLs).

Whole school approach

Whole school approaches always make teaching more effective than lessons alone. Our whole school approach goes beyond teaching to include all aspects of school life, including:

- culture
- ethos
- environment
- partnerships with families and the community

We embed teaching about online safety and harms within this approach by:

- having clear processes for reporting incidents or concerns in the child protection policy
- reflecting online behaviours in the school's behaviour and bullying policies
- ensuring our website is informative for parents and empowers them to keep their children safe

Engaging staff, pupils, parents and carers

We engage staff, pupils, parents and carers in school activities because working together to safeguard children is a collective responsibility. Our principles of online safety, and what we teach, are co-designed to reflect any emerging issues parents and pupils are hearing about or facing online

Reviewing and maintaining the online safety principles

We make sure that school staff have access to up to date appropriate training and resources so that they are confident in covering the required content in a way that is relevant to their pupils' lives by working with our IT provider.

Using information available to us, we also hold all practices under review to ensure we can respond to any issues our pupils are facing in a timely manner.

We embed our online safety principles by reinforcing what is taught in lessons by taking appropriate and consistent action when a pupil:

- makes a report of unacceptable online behaviours from another pupil, including cyberbullying

- shares a concern about something they have seen online

We expect the same standards of behaviour on and offline and support parents to reinforce and uphold these expectations at home (see website).

Filtering and Monitoring

The schools governing body must ensure that appropriate filters and monitoring systems are in place to safeguard children from potentially harmful and inappropriate online material, including when children are online at home. The school uses netsweeper, a filtering system which is a member of Internet Watch Foundation (IWF), signed up to Counter-Terrorism Internet Referral Unit list (CTIRU) and blocks access to illegal content including child sexual abuse material (CSAM). The system blocks around 292 categories and is applied to all users, including guest accounts, school owned devices and devices using the broadband connection. All mobile devices must be connected to the school network before they can be used.

The federations' filtering system:

- filters all internet feeds, including any backup connections
- is suitable for the age and ability appropriate for the users, and be suitable for educational settings
- can handle multilingual web content, images, common misspellings and abbreviations
- identifies technologies and techniques that allow users to get around the filtering such as VPNs and proxy services and block them
- provides alerts when any web content has been blocked (UK prevent alerts every 5 minutes).
- Identifies the device name or ID, IP address, and where possible, the individual
- the time and date of attempted access
- the search term or content being blocked

Lucy Howe, Headteacher, is the assigned member of staff on the federation leadership team responsible for:

- procuring filtering and monitoring systems
- documenting decisions on what is blocked or allowed and why
- reviewing the effectiveness of your provision
- overseeing reports

The school works with the IT provider to:

- procure systems
- identify risk
- carry out reviews and checks

School staff are responsible for reporting when:

- they witness or suspect unsuitable material has been accessed
- they can access unsuitable material
- they are teaching topics which could create unusual activity on the filtering logs
- there is failure in the software or abuse of the system
- there are perceived unreasonable restrictions that affect teaching and learning or administrative tasks
- they notice abbreviations or misspellings that allow access to restricted material

The school has effective monitoring strategies that meet the safeguarding needs of both schools. The monitoring system reviews all user activity on school and college devices by alerts and observations, allowing prompt action to be taken and responses recorded.

The school has identified that the risk profile of its pupils warrants physical monitoring and third party device monitoring to enable us to check whether incidents are malicious, technical, or safeguarding in nature, which are instantly addressed.

The school is working with its IT provider to ensure in meets all cyber security standards and Broadband internet standard.

Authorising Internet access

- All staff must read and sign the acceptable use of IT (code of conduct) before using school or mobile devices. In this policy, the use of mobile devices is clearly explained.
- Both schools will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- Any person not directly employed by the school will be asked to sign an 'acceptable use of school ICT resources' before being allowed to access the school's network
- Before pupils can access the network, written consent must be obtained from someone with parental responsibility for the pupil.

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the school can accept liability for any material accessed, or any consequences of Internet access, but we do expect all staff and pupils to report concerns.
- The school will audit ICT use to establish if the online safety policy is adequate and that the implementation of the policy is appropriate and effective.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.

Handling Online safety complaints

- Complaints of Internet misuse will be dealt with under the complaints policy.
- Any complaint about staff misuse must be referred to the Head teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure (see schools complaints policy)
- Pupils and parents will be informed of consequences for pupils misusing the Internet.

Introducing the policy to pupils

- e-Safety rules will be posted in all rooms where computers are used and discussed with pupils regularly.
- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.
- Instruction in responsible and safe use should precede Internet access.
- A programme of training in e-Safety, based on the materials from CEOP, is implemented, with particular units across both schools through PSHE and computing lessons
- Internet Safety Issues highlighted yearly within assemblies, special 'awareness' days and with letters/surveys to parents around Internet Safety
- Online safety is explicitly taught and embedded within the computing curriculum.

Staff and the policy

- All staff, including supply staff are signposted to this policy, with its importance explained.
- Staff understand how the filtering and monitoring systems work, and their roles and responsibilities related to these (see above)
- Staff always use a child friendly safe search engine (swiggle) when accessing the web with pupils.
- Staff will not use apps or sites which are blocked by the firewall

Enlisting parents' and carers' support

- Parents and carers attention will be drawn to the School policy in newsletters, the prospectus and on the school Website.
- The school maintains a list of e-safety resources and practical ideas for parents/carers on the school web site for the safe use of the Internet at home.

Regulation

The use of a finite and expensive resource, which brings with it the possibility of misuse, requires regulation. In some cases, access within both schools must simply be denied, for instance unmoderated chat rooms present immediate dangers and are banned. Fair rules, clarified by discussion and prominently displayed at the point of access, will help pupils make responsible decisions. The school works in partnership with parents, the LA, DfE and the Internet Service Provider (Hampshire) to ensure systems to protect pupils are reviewed and improved.

If staff or pupils discover unsuitable sites with inappropriate (containing adults) content the URL (address) and content must be reported to the Internet Service Provider via email. (Head teacher must also be informed immediately).

If staff or pupils discover unsuitable sites with illegal content the URL (address) and content must be reported to the Internet Service Provider via email. (Head teacher must be informed immediately). The computer concerned should be left connected to the site and the electricity disconnected (the police have requested this to help investigation work). The base unit then needs to be secured for police collection, if necessary.

Staff should be aware that internet traffic and inappropriate use of Internet facilities will be monitored (by LA, ICT co-ordinator and the Senior Management Team) and traced to the individual user. Discretion and professional conduct is essential.