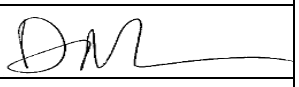
HEBBURN
Comprehensive School

WORK HARD | BE KIND | ASPIRE

E-Safety Policy

Review Period	Recommended Annually		
Date of next review	Spring Term 2027	Author(s)	Mrs S Burdis
Type of Policy	Statutory	Approval	Governing Body
Signed by:			
Head Teacher	Mr D Thompson	Date: 17 February 2025	
Chair of Governors	Mr G Thompson	Date: 17 February 2025	

Vision and Values

Our vision at Hebburn Comprehensive School is to have a harmonious community where the emphasis for all is on learning and achievement, where pupils feel safe and where a culture of success and ambition is celebrated and embedded throughout the school and wider community. We aim to raise the aspirations of all our young people, inculcating a respect for one another and for the value of learning and citizenship. Through challenge, partnership and support, we aim to raise standards of achievement; create a genuine sense of community spirit; and enhance our pupils' life chances for the future.

All children deserve the opportunity to achieve their full potential. At Hebburn Comprehensive School, we have a commitment to securing the five outcomes set out below:

- Be healthy
- Stay safe
- Enjoy and achieve
- Make a positive contribution

**** It is the responsibility of all staff to read through this document and be fully aware of its contents. If any issues do arise in the future, failure to have read this policy and not being familiar with its contents cannot be used as a reason for not adhering to procedures.****

Rationale

1) **Definition and Usage**
2) **Part Managed Service**
3) **Use of Information and Communication Technologies <u>for Staff</u>**

   Acceptable Use Policy

   A. Data Security
   B. Passwords
   C. Internet Usage
   D. E-mail
   E. Filtering and Monitoring
   F. Social Networking
   G. Mobile Devices
   H. Filtering and Monitoring and Reporting
   I. Reporting Accidental Access
   J. Reporting Deliberate Abuse or Misuse
   K. Cyber-Bullying

4) **Use of Information and Communication Technologies <u>for Pupils</u>**

   Acceptable Use Policy

   A. Passwords
   B. Internet Usage
   C. E-mail
   D. Social Networking
   E. Mobile Devices
   F. Monitoring and Reporting
   G. Reporting Accidental Access
   H. Reporting Deliberate Abuse or Misuse
   I. Cyber-Bullying
   J. Sanctions for misuse

5) Appendix

A. Dealing with an e-safety incident
B. Reporting an e-safety incident - guidance
C. Committing an illegal act

Rationale

The safeguarding and well-being of all pupils at Hebburn Comprehensive School are of paramount importance.

The purpose of this document is to:

- Help ensure that all pupils and staff can work online confidently and safely, maintaining the professional standards and expectations of the school.

- Ensure that all pupils and staff have a clear understanding that illegal, inappropriate and unsafe behaviours are unacceptable and may well result in disciplinary action/sanctions.

1. Definition and Usage

This policy applies to all users of the school's ICT facilities, whether in school or connected remotely, from home or elsewhere. This includes all users, whoever they are, whatever technology is used, whenever and wherever they are, if connected to the school network.

It is the responsibility of all users of the school ICT facilities to be aware of and follow all school ICT policies and guidelines contained in this document. It is also the responsibility of all users of the school ICT facilities to seek advice, in case of doubt, from the E-safety Officer, Mrs Burdis.

2. Part-Managed Service

ICT facilities at Hebburn Comprehensive School are maintained by the Network Manager and other IT support staff and where necessary, in the case of illness, the need for cover support is provided by an external service provider.

3. Use of Information and Communication Technologies <u>for Staff</u>

Acceptable Use Policy

A. Data Security

- Networked computers are a critical asset to the school and must be managed carefully to maintain security, data integrity and efficiency.

- Software purchased by the school, which has been tested and installed by the school technician, may be used on the school network. ***Non-standard or unauthorised software must not be installed on the school network.***

  The installation of copied software on the network is <u>not</u> authorised under any circumstances.

- Under no circumstances should members of staff disclose personal or other confidential information held on a computer or the school network (e.g. information contained in Bromcom) to unauthorised

persons. The unauthorised access to and/or unauthorised modification of data is a criminal offence under the Computers Misuse Act 1990.

- It is school policy to store data on regularly backed-up network drives and cloud. Members of staff should ensure that data that is not stored on the network is regularly backed-up.

- Anti-virus software is installed on all computers as standard and is updated regularly via the network. Files received or sent by e-mail are checked for viruses automatically.

- Users are strictly forbidden to intentionally access or transmit computer viruses.

- When a member of staff suspects that a virus has infected a computer, the Network Manger should be informed immediately.

- The school do not allow the connection of external computer equipment to the network, other than external hard drives or memory sticks via USB ports.

B. Passwords

Passwords protect school computers and networks from access by unauthorised people: they protect the work of staff and pupils as well as school information, some of which may be sensitive and confidential. Therefore, users should be careful to safeguard their password at all times. Passwords should never be shared with anyone, even trusted people.

As per the school's managed service regulations, staff will be requested to change their log-in password regularly, and they are required to use a complex password with letters, characters and numbers.

C. Internet Usage

The overriding principle guiding the use of the internet is that it must not breach professional standards that are essential and expected in a school responsible for the education, well-being and safeguarding of children and young people.

Access to the Internet in school is **not for private use**. The Internet must only be used for educational purposes (e.g. accessing school e-mail and the Portal, downloading and making learning resources, etc.)

Material regarded as offensive under English law must not be accessed or published on the Internet. Such material would include content concerning sex, race, colour, religion, national origin, sexual orientation or disability. Deliberate access or publishing of offensive material would constitute misconduct and would invoke the school's disciplinary procedures and a possible criminal investigation. Copyright and licensing conditions must be observed when downloading software or other material from the internet.

All Internet usage from the school network is systematically monitored and logged.

D. E-mail

- The school's e-mail system is provided for school business purposes only.
- There is no obligation to respond to emails outside of working hours.
- All staff e-mail messages should only be sent when the content is appropriate and relevant to all recipients.
- E-mail messages cannot be considered to be private, confidential, secure or temporary.
- Improper statements and attachments in e-mail communication can give rise to personal liability, as well as liability for the school, and can constitute a serious disciplinary matter.
- E-mail messages that may be defamatory, intimidating, hostile or offensive on the basis of sex, race, colour, religion, national origin, sexual orientation or disability must not be sent. Should you receive such e-mail, always report it to the E-safety Officer.
- Copyright law applies to e-mail.
- It is not permissible to access or to send e-mail from another user's personal account.
- Further guidance on the suitable use of e-mail is available in Appendix C.

E. Filtering and Monitoring

All school owned computers and IT systems must be authenticated and passed though the firewall and web filter when accessing the internet, and filtered at the appropriate level.

Any bring your own devices (BYOD) must also be authenticated by a user and apply the appropriate level of filtering and monitoring and therefore no communication over this service should be considered private or protected. If requested to do so by authorities, we may disclose information about you and use of service. This service may be blocked suspended or teminated at any time for reasons not limited to, violation of this policy, disruption of access to other users or any other violation of applicable laws and regulations.

Attempts to access banned sites will result in users being reported to the E-safety Officer and the appropriate authority being notified (see Appendix A).

Accidental access to banned sites must be reported to the E-safety Officer immediately and logged.

Whilst it is essential that appropriate filtering and monitoring systems are in place, school will ensure that "over blocking" does not lead to unreasonable restrictions as to what pupils can be taught with regard to online teaching and safeguarding.

School will ensure appropriate filtering and monitoring on school devices and school networks, taking the areas of risk as categorised by the 4Cs into consideration:

Content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.

Contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

Conduct: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and

Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

School will do all that they reasonably can to limit children's exposure to the above risks from the school's IT system. They will ensure that school has appropriate filtering and monitoring systems in place and will regularly review their effectiveness. They will ensure that the leadership team and relevant staff have an

awareness and understanding of the provisions in place and manage them effectively, escalating concerns when necessary, as identified below. All staff should receive appropriate safeguarding training, including online safety which includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring. School will consider the number of and age range of pupils, those who are potentially at greater risk of harm and how often they access the IT system along with the proportionality of costs versus safeguarding risks.

School will:

- identify and assign roles and responsibilities to manage filtering and monitoring systems
- review filtering and monitoring provision at least annually
- block harmful and inappropriate content without unreasonably impacting teaching and learning
- have effective monitoring strategies in place that meet their safeguarding needs.

F. Social Networking

- Social networking sites have become a part of everyday life and have huge advantages; however, working with young people brings a set of responsibilities that staff are strongly advised to note: **pupils <u>must never be</u> online 'friends'.** Adding pupils as 'friends' on a personal social networking site is ***not appropriate.*** This also applies to ex-pupils who have left the school.

There has been a lot of press coverage in recent years, relating to issues with social networking and young people. Whilst the school is not suggesting that any member of staff would put themselves in a vulnerable position, it must be stressed that there are cases nationally, where allegations have been made against staff working in schools, which have caused a great deal of distress for all parties involved.

The school would not wish to see anyone placed in a situation where they could be vulnerable to allegations, so the following guidance is offered:

- **Protect your information:** It is advisable to have privacy settings on your account to restrict access to personal information (be aware that this still does not guarantee privacy).
- **Be mindful about what you are publishing and the potential audience:** Although privacy controls may be set, the information could still be shared. It is sensible to think that, once published, the information is no longer private.
- **Be professional:** Do not discuss your school, colleagues, parents or pupils on social networking sites, as this could lead to potential issues.

G. Mobile Devices

School mobile phones are available for any activities taking place offsite, where staff may need access to a mobile phone.

Personal mobile phones (staff) should be kept secure at all times. In classrooms, mobile phones should be turned off or set to silent/vibrate. [TO REMOVE – phone are used by staff now for emails/key communication?]

Personal mobile devices **must not** be used to take photographs, videos or sound clips of pupils. Dedicated school cameras and mobile devices are available, on a sign-out basis, from the main office / IT Support Office and should be the only devices used to take pictures or videos of pupils. Staff should ensure that permission has been given and that permission forms have been signed before taking pictures of children.

When returned, photographs will be downloaded to the school system and stored in clearly labelled folders, where they will be accessible to staff only. Subsequently, all images will be deleted before these cameras can be used again by other members of staff.

It is absolutely vital that parental permission is obtained before any pictures of a child are published, whether internally or externally. It is also essential, when publishing images of children, that there is no link between a particular picture and the names of the children shown within that picture.

H. Filtering and Monitoring and Reporting

Network and internet usage by staff is monitored robustly by the Designated Safeguarding Lead and Network Manager. Key members of the pastoral team monitor pupil usage of the network and internet. All filtering and monitoring is carried out using an enterprise grade firewall with appropriate filtering, reporting tools and monitoring software meeting the DfE filtering and monitoring standards. A log is kept of all sites visited. Any violations identified will result in further investigation, may be reported to the Local Authority, and may lead to disciplinary and/or criminal action.

I. Reporting Accidental Access

Any member of staff who accidently comes across illegal material should do the following:

- Report the incident to the E-Safety Officer and the Safeguarding Officer, or in their absence, the Deputy Head Teacher, who will log the incident.
- Not show anyone the content or make public the address of the website containing the illegal material

The E-Safety Officer will follow the guidelines in Appendix A, "Dealing with an E-Safety Incident".

J. Reporting Suspected Deliberate Abuse or Misuse

Any member of staff suspecting another person of deliberate misuse or abuse of the school network should take the following action:

- Report, in confidence, the incident to the E-Safety Officer and/or the Safeguarding Officer (Mrs Burdis), or in their absence, directly to the Head Teacher.
- The Head Teacher may inform the Local Authority, if necessary.
- The E-Safety Officer and an additional member of the safeguarding, or leadership team will complete an internal investigation.
- If the investigation results in confirmation of access to illegal materials or the committing of illegal acts, the school will inform the police and a criminal investigation may follow.
- The school's disciplinary procedures will be followed by the Head Teacher.

Further Guidance is available in Appendix B, "Reporting an E-Safety Incident – Guidance"

4. Use of Information and Communication Technologies <u>for Pupils</u>

Acceptable Use Policy

A. Passwords

Passwords protect the school's systems from access by unauthorised people.
Pupils should only access the system with their own log-in ID and password, which **must be kept secret**.

Passwords will be required to be changed regularly.

Pupils must never use anyone else's password.

Should pupils never leave their computer unattended, it is their responsibility to ensure they lock their desktop.

B. Internet Usage

- All Internet usage from the school network is logged and monitored.
- Pupils must only access the Internet using their own log-in details.
- Internet usage is for the purpose of learning.

The following are strictly forbidden:

- Using the Internet to download, send, print, display or otherwise gain access to materials which are unlawful, obscene or abusive.
- Posting or uploading images of other people using school ICT facilities.
- Attempting to change or by-pass the filtering and security systems on devices belonging to the school, either on the school premises or from home.
- Arranging to meet someone or give any personal information over the Internet while in school.

C. E-Mail

- The school's e-mail system is provided for learning purposes only.
- All e-mail messages should only be sent when the content is appropriate and relevant to the recipient(s).
- E-mail messages cannot be considered to be private, confidential, secure or temporary.
- Improper statements in e-mail can give rise to a serious disciplinary matter.
- E-mail messages that may be defamatory, intimidating, hostile or offensive on the basis of sex, race, colour, religion, national origin, sexual orientation or disability must not be sent. Should pupils receive such e-mail, they must report it a member of staff.
- Copyright law applies to e-mail.
- It is not permissible to access or to send e-mail from another pupil's personal account.

D. Social Networking

Social networking websites must not be accessed in school.

Should pupils access social networking sites in their own time, they should bear in mind that:

- There are no privacy settings that truly protect anyone's privacy.
- Comments and images posted on social network sites are on the Internet forever.
- Things said online can be taken and shared with other people, sometimes out of context. This can be dangerous.

The following guidance is offered:

- **Protect your information:** Make sure you understand the privacy settings and can restrict access to information you consider personal (be aware that this still does not guarantee privacy).
- **Think about what you are publishing:** Although you may have set strict privacy controls, the

information could still be shared by one of your 'friends'. It is sensible to think that, once published, the information is no longer private.

- **Watch who comments:** Although you might be careful with what you are posting, it is possible that you may receive inappropriate comments, pictures or videos from your contacts.
- **Protect your image**.
- **Never arrange to meet anyone through a social networking site.**

E. Mobile Devices

Hebburn Comprehensive takes no responsibility for the security of any type of mobile device.

Whilst the school does recognise that, for safeguarding reasons, parents may wish for their children to have mobile phones with them for contact on the way to and from school, **they must not be used at all during the school day, including lunchtime.**

- Mobile phones/electronic devices **must not** be used, at any time, for videoing or taking pictures.
- Phone should be switched off and out of sight.
- If a phone rings/beeps 'accidently' (has been left switched on), pupils will be told to switch it off and the phone will be confiscated.
- Should a mobile phone/electronic device cause disruption to learning during a lesson (pupil has it out when they shouldn't), it will be confiscated and placed in the main office. If this is deemed to be sufficient for that particular incident, it will be returned to the pupil at the end of the school day. A C2 will be issued.
- If a pupil's mobile phone/electronic device causes persistent problems, the Head of Learning may decide to confiscate it until a parent or carer comes to collect it from school.
- If a pupil is requested to hand a mobile phone/electronic device over and refuses to do so, they will be taken to a HoD, HoL or a member of the SLT. Should the pupil persist in refusing to hand over their mobile phone, parents/carers will be contacted to help resolve the matter. This will be followed by a placement in the BSR and could result in a suspension.
- If pupils follow the advice of not having mobile phones/electronic devices out and having them switched to silent mode, there should not any issues.

F. Monitoring and Reporting

Network and Internet usage is monitored and a log is kept of all sites visited. Any pupil misusing the system will have internet, e-mail and network access suspended. Sanctions for misuse may apply.

G. Reporting Accidental Access

Any pupil who accidentally comes across inappropriate material should report the incident to their teacher **immediately**.

H. Reporting Suspected Deliberate Abuse or Misuse

Any pupil suspecting another person of deliberate misuse or abuse of the school network should inform their teacher **immediately**.

I. Cyber-Bullying

Cyber-bullying involves the use of new information and communication devices and services, including e-mail, instant messaging, text messages, mobile phones and social networking websites to bully, harass or intimidate an individual or group of young people.

The school takes all cyber-bullying incidents very seriously, and deals with all incidents according to the school's Anti-bullying and Behaviour Policies.

All suspected incidents of cyber-bullying should be reported to the E-safety Officer/Safeguarding Officer, Mrs S Burdis.

Further information can be found in the school's Cyber Bullying, Anti-bullying and Behaviour Policies.

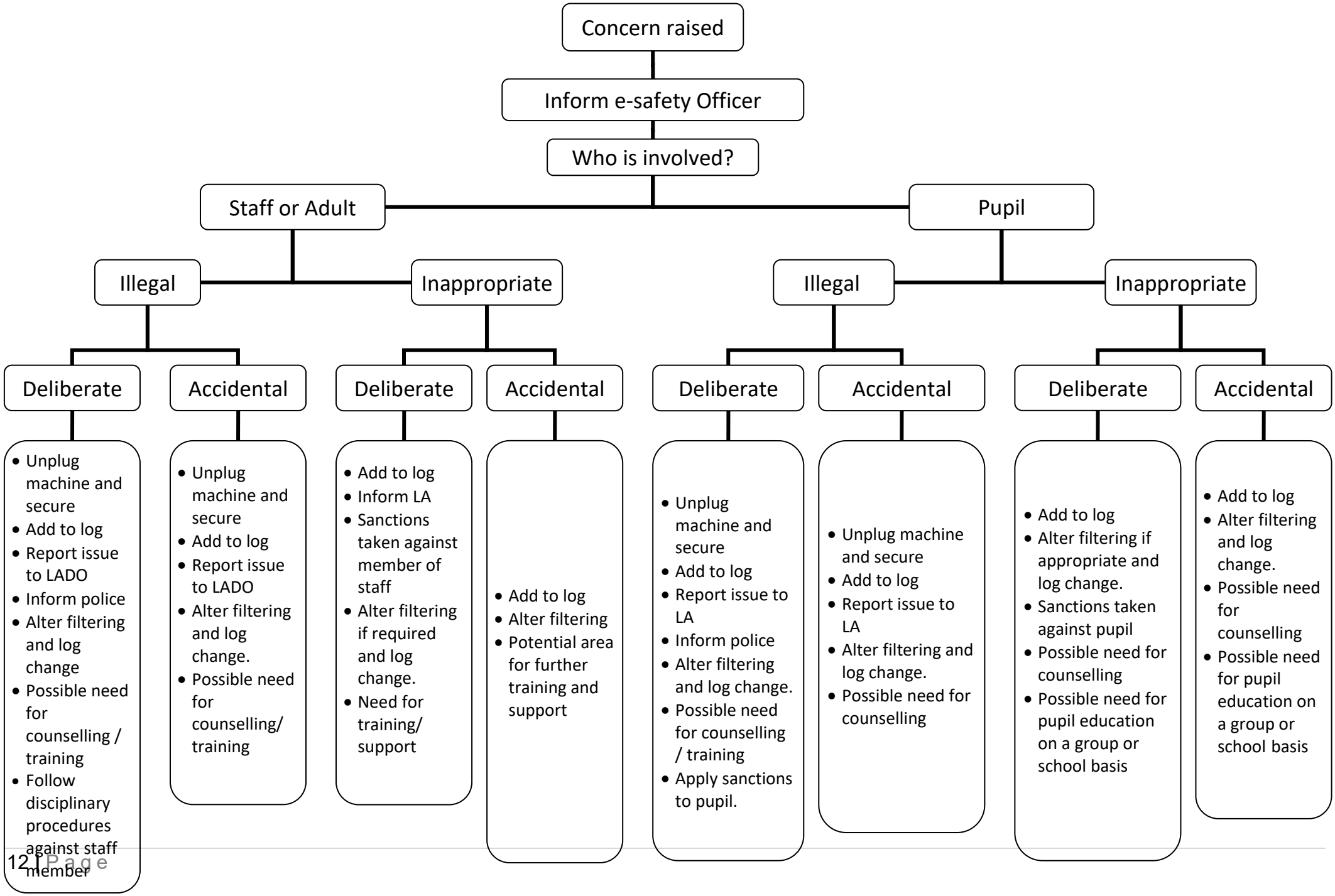
J. Sanctions for Misuse

The school wishes to promote the highest standards in relation to good practice and security in the use of information technology.

- Sanctions may result in a temporary or permanent ban from use of the Internet/computer.
- Parents/carers will be informed.
- Behaviour policy sanctions will be applied for use of inappropriate language or behaviour.
- If necessary, external agencies and the police may be contacted and informed.

Appendix A

Dealing with an E-Safety Incident


Concern raised
Inform e-safety Officer
Who is involved?
Staff or Adult
Pupil
Illegal
Inappropriate
Illegal
Inappropriate
Deliberate
Accidental
Deliberate
Accidental
Deliberate
Accidental
Deliberate
Accidental
• Unplug machine and secure
• Add to log
• Report issue to LADO
• Inform police
• Alter filtering and log change
• Possible need for counselling / training
• Follow disciplinary procedures against staff member
• Unplug machine and secure
• Add to log
• Report issue to LADO
• Alter filtering and log change.
• Possible need for counselling/ training
• Add to log
• Inform LA
• Sanctions taken against member of staff
• Alter filtering if required and log change.
• Need for training/ support
• Add to log
• Alter filtering
• Potential area for further training and support
• Unplug machine and secure
• Add to log
• Report issue to LA
• Inform police
• Alter filtering and log change.
• Possible need for counselling / training
• Apply sanctions to pupil.
• Unplug machine and secure
• Add to log
• Report issue to LA
• Alter filtering and log change.
• Possible need for counselling
• Add to log
• Alter filtering if appropriate and log change.
• Sanctions taken against pupil
• Possible need for counselling
• Possible need for pupil education on a group or school basis
• Add to log
• Alter filtering and log change.
• Possible need for counselling
• Possible need for pupil education on a group or school basis

Appendix B

Reporting an E –Safety Incident
Guidance

Introduction

E-safety incidents can take many forms, from the accidental access of inappropriate content, to serious incidents, including illegal images or behaviours by adults or children.

Schools need to be clear in their understanding of the differences between **'inappropriate'** and '**illegal'** content. Examples of **inappropriate** content can include soft porn, political extremism and online gaming, whilst **illegal** content is defined by the Internet Watch Foundation as 'child sexual abuse content hosted worldwide and criminally obscene and incitement to racial hatred content hosted in the UK'.

Adults (including teachers, support staff, governors, visitors)

Where **illegal** content is accessed deliberately or accidentally, the incident needs to be logged, reported to the Head Teacher and the LADO. Where the incident is believed to be deliberate, the school must also notify the police but must ensure that the Local Authority is informed first.

Although **illegal** sites are filtered, it is unlikely that either a child or an adult will access them accidentally. Having said this, there *is* a possibility that an illegal site not yet listed with the Internet Watch Foundation is not filtered and a genuine accidental incident could occur. In some extreme cases, the police may need to be informed of accidental access to illegal material; the Local Authority contact will advise schools on the appropriateness of this action when the incident is reported to them.

In either accidental or deliberate cases, the equipment will need to be isolated and the Local Authority or police will arrange for forensic examination of the device. The Local Authority will provide assistance in adjusting the in-school filtering and provide further training, support and guidance.

Where **inappropriate** content is accessed accidentally, the filtering policies can be amended and further training and support provided, if required. In the case of deliberate access, the school should follow established disciplinary procedures, amend filtering and notify the Local Authority.

Children and Young People

The reporting processes remain the same as those for incidents relating to adults. Where **illegal** activity has taken place accidentally or deliberately, the device needs to be isolated, forensically analysed and restored prior to using again within the establishment.

In the case of either deliberate or accidental access to **illegal** content, it is likely that the person will need counselling and support within school and other agencies. The Local Authority will be able to assist with identifying this.

Where a child or young person has deliberately or accidentally accessed **inappropriate** content, there is an opportunity to provide further education to the individuals involved and the pupils. Your Local Authority can provide in-school support and provide information on other sources of information and teaching and learning resources.

In each instance, it is important to ensure that parents and carers are aware of the incident and encouraged to support the school's actions.

Appendix C

COMMITTING AN ILLEGAL ACT

1 Receiving unsolicited emails that may contain potentially illegal material (either as an attachment or in a URL) is not an illegal offence.

2 If you receive potentially illegal material you could easily commit an illegal act - **do not open the material or investigate personally.**

3 Opening an attachment or URL that proves to hold illegal content **is an illegal act** and is classed as possession of illegal material.

4 Showing anyone else illegal material that you have received **is an illegal act.**

5 Printing a copy of the offensive email to report it to someone else **is an illegal act** and is classed as producing illegal material.

6 Printing a copy of the material to give to someone else **is an illegal act** and is classed as distributing illegal material.

7 Within 4 simple steps you could easily break the law 4 times. Each is a serious offence.

8 **Never** open unsolicited URLs or attachments. If you are suspicious that the content could be illegal report it and log that you have received it.

9 Always report potential illegal content to the Internet Watch Foundation at www.iwf.org.uk They are licensed to investigate: **you are not.**

Never investigate personally.
If you open illegal content accidentally, report it to the school's E-safety Officer/Safeguarding Officer/ Head Teacher.
Do not copy and paste the URL into an e-mail, write it down. This prevents accidental opening.
Once the e-mail has been reported and logged, delete it from your inbox.
If you are unsure, contact the Internet Watch Foundation for advice.