

HEBBURN COMPREHENSIVE SCHOOL



E-SAFETY POLICY [E-Safety Officer: Mr D Perez]

Approved by Governors: December 2009

Review Date: June 2011

1) Rationale

2) Definition and Usage

3) Use of Information and Communication Technologies for Staff Acceptable Use Policy

- A. Monitoring and Reporting
- B. Reporting Accidental Access
- C. Reporting Deliberate Abuse or Misuse
- D. E-mail
- E. Internet Usage
- F. Social Networking
- G. Video Conferencing
- H. Passwords
- I. Mobile Devices
- J. Cache Pilot
- K. Cyber-Bullying
- L. Disciplinary Action

4) Use of Information and Communication Technologies for Pupils Acceptable Use Policy

- A. Monitoring and Reporting
- B. Reporting Accidental Access
- C. Reporting Deliberate Abuse or Misuse
- D. E-mail
- E. Internet Usage
- F. Social Networking
- G. Passwords
- H. Mobile Devices
- 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
- D. What to do with Suspicious E-mail

1. Rationale

The purpose of this document is to:

- Help ensure that all adults and pupils can work online confidently and safely, whilst maintaining the professional standards and expectations of the school.
- Ensure that all adults and pupils have a clear understanding that illegal, inappropriate and unsafe behaviours are unacceptable and may well result in disciplinary action/sanctions.

2. Definition and Usage

This policy applies to all users of the school network, 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 network.

3. Use of Information and Communication Technologies for Staff Acceptable Use Policy

A. Monitoring and Reporting

Network and Internet usage is monitored and a log is kept of all sites visited. Any violations identified will result in further investigation, will be reported to the Local Authority and may lead to disciplinary and/or criminal action.

B. Reporting Accidental Access

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

- Report the incident to the E-Safety Officer, or in his absence, to the Network Manager.
- Not show anyone the content or make public the URL.
- Make sure that the incident is logged.

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

C. 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, or in his absence, directly to the Head Teacher.
- The Head Teacher should inform the Local Authority.
- Two senior members of staff - not the Head Teacher - 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"

D. E-mail

- The school's e-mail system is provided for the school's business purposes.
- All staff e-mail messages should only be sent when the content is appropriate to the recipient(s) and of relevance to staff.
- E-mail messages cannot be considered to be private, confidential, secure or temporary.
- Improper statements in e-mail can give rise to personal liability and 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 should not be sent. Should you receive such e-mail, always report it to the E-Safety Officer.
- Attachments should only be opened if they come from a known and trusted source: if in doubt, contact the Network Manager.
- Copyright law applies to e-mail.
- It is not permissible to access or to send e-mail from another employee's personal account.
- Further guidance is available in Appendix D "What to do with Suspicious E-mails".
- Guidance on what constitutes illegal acts is available in Appendix C, "Committing an Illegal Act – Did You Know?"

E. Internet Usage

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

The Internet is **not for private use during working hours.**

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 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 monitored, logged and randomly checked.

Parental permission must be obtained before any pictures of a child are published, whether on an internal or external site. It is 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.

F. Social networking

Social networking is second nature to many colleagues who have spent much of their youth texting and using instant messaging. Social network sites are used by people of all ages and millions of people worldwide use them every day.

However, staff should bear in mind that:

- There are no privacy settings that truly protect your privacy.
- Comments and images posted on social network sites are on the internet for ever – even after you delete them from your account.
- Things you say can be taken and shared, sometimes out of context, with employers, colleagues, parents and children.

Colleagues should always remember that information published on their site may be read by colleagues, parents or pupils. To prevent any misunderstanding, the following guidance

is offered:

- **Separate personal from professional:** Decide from the start how you will use your account and the sort of information it will contain. If appropriate, you could create two different accounts.
- **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.
- **Be professional:** Do not, under any circumstances, discuss your school, colleagues, parents or pupils.
- **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: this is beyond your control.
- **Protect your image.**
- **Talk to your friends and contacts:** If it is a personal site, they should understand the need to keep your information private and not post inappropriate or potentially embarrassing comments, pictures or video footage on an open site. If it is a professional site, they need to understand why you may not add them as friends or, if added, the types of posts or comments that are acceptable.
- **Pupils must never be online friends:** It is highly inappropriate and potentially dangerous, to add pupils as friends on a personal site and the same could apply to parents. If you are looking to engage with the school community online then consider setting up a school account that can be open and managed by several members of staff. For advice, contact the E-Safety Officer.

G. Video Conferencing

Video Conferencing should only take place in the presence of a member of staff, in the Learning Resource Centre. Sites should only be accessed via the JANET Videoconferencing Service.

H. Passwords

Passwords are crucial to the security of PCs, Network and individuals. Passwords should never be shared with anyone, even trusted people. It is strongly recommended that passwords are changed regularly and contain letters, characters and numbers. Passwords should never be saved, on any computer.

I. Mobile Devices

Personal mobile phones should not be used for work purposes. School mobile phones are available for any activities taking place offsite where staff may need access to a mobile phone: please see the Business Manager, Mrs McGregor.

Staff mobile phones should be kept secure at all times, especially when they contain personal information. Mobile phones suspected of being stolen should be reported to the Police.

In classrooms, mobile phones should be turned off or set to silent/vibrate.

Bluetooth technology should be **kept off**, to prevent others from sending content or messages that may be inappropriate or illegal.

Laptops are provided for school business. The private use of laptops outside of school hours is permissible. Staff need to be aware that they are responsible for any files viewed or downloaded on their laptop. In the last half term of the academic year, all laptops must be returned for one day, for servicing and vetting by the Network Manager.

Mobile devices must not be used to take photographs, video or sound clips of any person who is unaware of the action and who has not given their permission. The use of personal equipment to take pupils' photographs is not allowed. Only school equipment should be used to take pictures or videos of pupils. Staff should ensure that permissions have been given and that permission forms have been signed before taking pictures of children. All images on cameras/phones must be deleted before the equipment is taken offsite. Images should be downloaded to the school secured shared area by ICT support staff, and stored in a clearly-labelled folder. Equipment must not be available for further use until images have been transferred/deleted.

J. Cache Pilot

All school computers must be authenticated and directed through the cache pilot, which contains set-up lists of approved sites. Attempts to access banned sites may result in the user's being reported to the appropriate authorities. Accidental access to banned sites must be reported to the E-safety Officer immediately and logged.

K. Cyber-Bullying

The DCSF has produced comprehensive advice on Cyber-Bullying as part of the Safe to Learn guidance. It can be accessed online from www.digizen.org/cyberbullying. All suspected incidents of cyber-bullying should be reported to the E-safety Officer.

L. Disciplinary Actions

The school wishes to promote the highest standards in relation to good practice and security in the use of information technology. Consequently, it expects and supports the professionalism and integrity of its staff. Where deliberate misuse has occurred, disciplinary sanctions will be applied.

In exceptional circumstances, where there are reasonable grounds to suspect that a member of staff has committed a serious criminal offence, the police will be informed and a criminal prosecution may follow.

4. Use of Information and Communication Technologies for Pupils Acceptable Use Policy

A. 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 and Network access stopped. Sanctions for misuse may apply.

B. Reporting Accidental Access

Any pupil who accidentally comes across inappropriate material should report the incident to their teacher **immediately**: not to do so could be thought of as an attempt to 'cover up' the issue.

C. 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**.

D. E.mail

E-mail messages cannot be considered to be private.
Messages sent via the school e-mail system should be polite and responsible.
Any unpleasant messages received should be reported to members of staff.
Posting anonymous messages and forwarding chain letters is forbidden.

E. Internet Usage

All internet usage from the school network is monitored and logged.
You must only access the Internet using your own login details.
Pupils are responsible for good behaviour on the Internet. Access is a privilege, not a right and that access requires you to show responsibility and maturity.

There is no reason connected to your school work that would ever need you to enter social networking sites or chat rooms. If you do so outside of school, remember that personal information should **never** be passed on over the Internet, and pupils **must never** arrange to meet anyone contacted through one of these sites. Always keep your parents informed.

F. Social networking

Social networking is used by many pupils out of school.

However, pupils should bear in mind that:

- There are no privacy settings that truly protect your privacy.

- Comments and images posted on social network sites are on the internet for ever – even after you delete them from your account.
- Things you say 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.**

G. Passwords

Passwords protect the school's systems from access by unauthorised people. Pupils should only access the system with their own login ID and password, which **must be kept secret**. Passwords should be changed regularly. You must never use anyone else's password.

H. Mobile Devices

Pupils' mobile phones should not be used in the building. In classrooms, mobile phones should be turned off or set to silent/vibrate.

When taking a public examination, all pupils must hand in to supervisors/invigilators any mobile device.

Bluetooth technology must be kept off.

Mobile devices must not be used to take photographs, video or sound clips of anyone.

MP3 players must not be used in the building, and must not be visible once a pupil enters the building.

Memory sticks should not be connected to the school network unless permission has been granted by a member of staff.

Mobile phones can be confiscated by members of staff and returned according to the policy.

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.

Further information can be found in the school's 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 will result in a temporary or permanent ban from use of the Internet/computer.

Parents/carers will be informed.

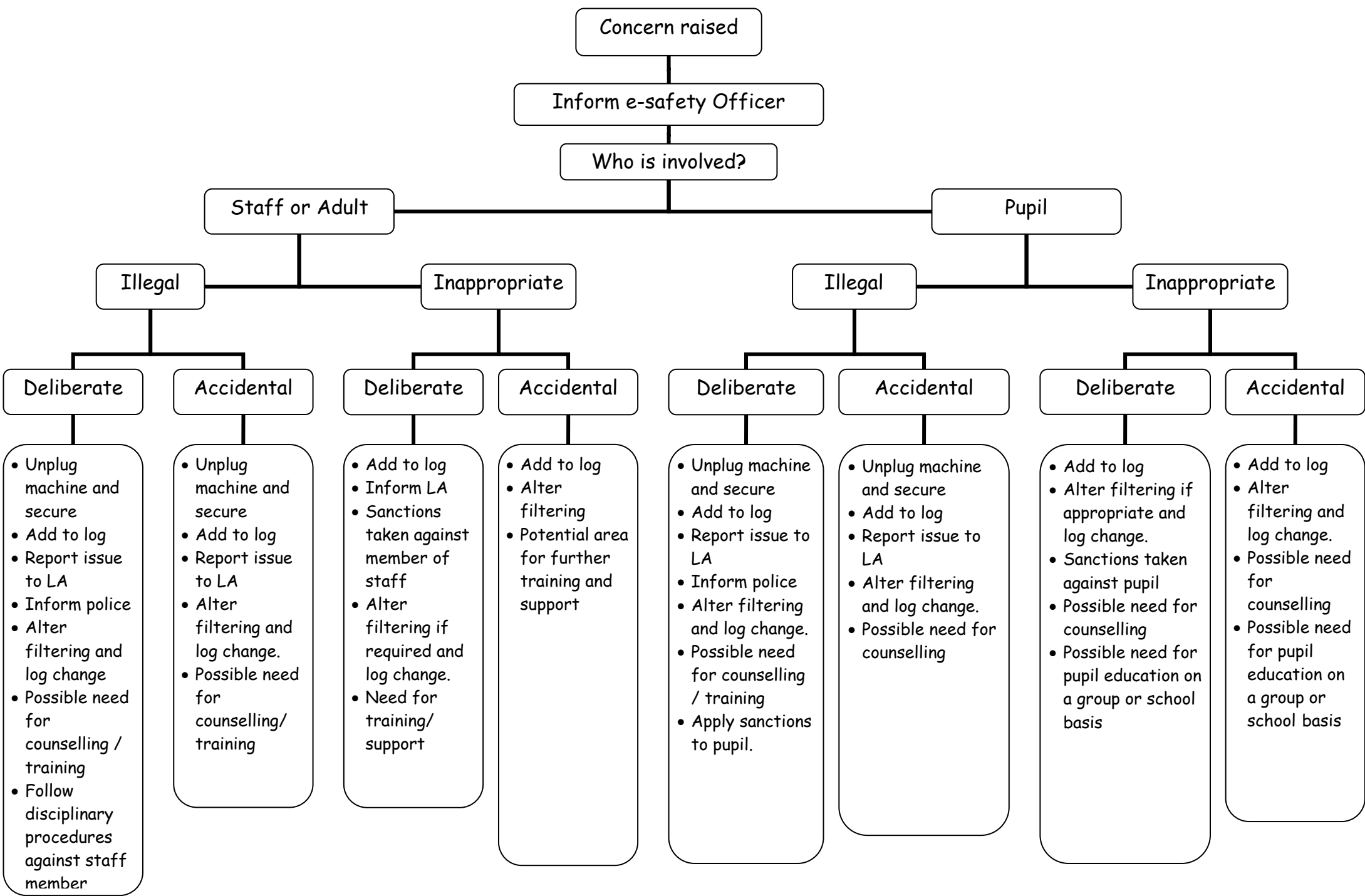
Behaviour policy sanctions will be applied for use of inappropriate language or behaviour.

If necessary, external agencies such as Social Networking or E-mail member sites may be contacted and informed.

If necessary, the police may become involved.

Dealing with an E-Safety Incident

Final Version April 2009 v3



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 LA
- 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 LA
- 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

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 (e.g. ‘page three’ images), 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 etc.)

Where **illegal** content is accessed deliberately or accidentally, the incident needs to be logged, reported to the Head Teacher and the Local Authority. 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, it *is* a remote 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.

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

4

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

7

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

2

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

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

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.

3

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

6

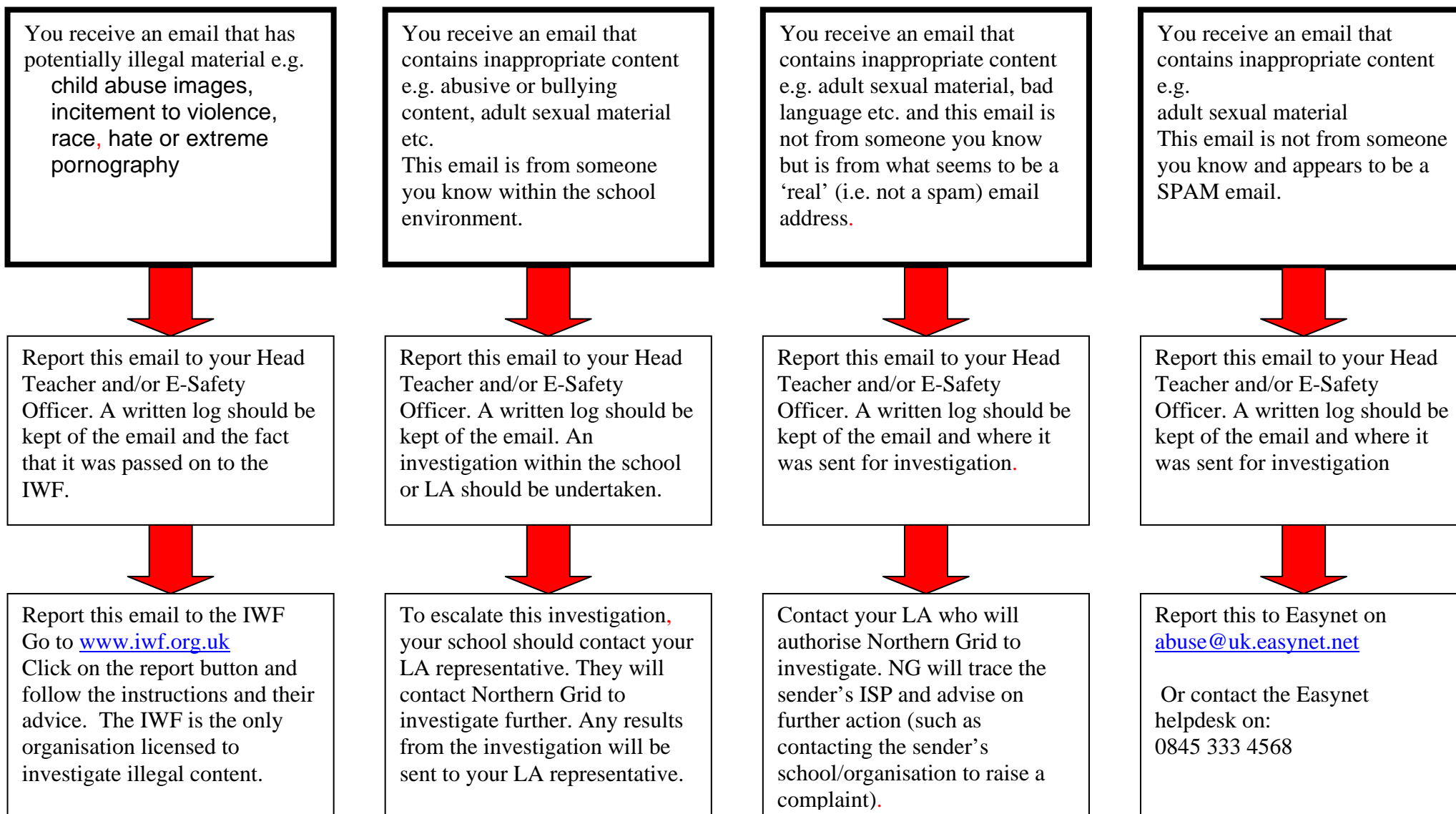
Printing a copy of the material to give to someone else **is an illegal act** and is classed as distributing illegal material

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 Head Teacher and IWF. Go to the IWF website and click on the report button. **Do not copy and paste the URL, write it down and type it into the reporting screen. This prevents accidental opening.** Once the email has been logged and reported to the IWF delete it from your inbox. If you are unsure, contact the IWF for advice on 01223 237 700. **The Internet Watch Foundation only deals with illegal content: please see their website for information and advice. Please note this guidance only relates to illegal content, not to inappropriate content.**

What to do with Suspicious Email



In all cases, secure the email in a folder and only delete when the investigation has been completed or you are advised to do so.

In the case of potential illegal material do not show the content of this email to anyone: report it to your Head Teacher and take the advice of the Internet Watch Foundation.

Do NOT always presume that the sender's email address is telling you the truth – Spammers can, and do, fake others' email addresses. If you are unsure how to proceed, please contact the Northern Grid for Learning on 0191 4611844.