How Pupils Should Report E-Safety Incidents in School

Rationale:

As part of e-safety education, all children should be taught how to report content on the internet which is a concern. Guidance should be available at all times, and although Ofsted will expect evidence that pupils know how to report material, teachers and support staff should be competent in offering guidance should an e-safety event occur.

It is well worth explaining to the children what will happen as a result of them reporting a concern. This empowers the pupils, and improves confidence that their concern will be taken seriously. It also provides an opportunity and forum to discuss hypothetical situations, and may well result in issues being uncovered which can then be dealt with in a sympathetic and secure setting.

E-safety Support

How pupils should report e-safety incidents in school

Tell a member of school staff:

In the first instance, a common sense approach should be taken when teaching pupils how to report e-safety concerns and incidents. Children should be encouraged to inform an adult promptly, and this can include any school staff.

The onus on procedure is then placed upon the staff members, who should all have adequate training with regard to documenting and reporting incidents. Normally this will involve invoking procedures as outlined in the school's e-safety policy – ie reporting to the school's e-safety officer; or if child protection issues are involved, following the school's child protection policy. Child protection policy and procedures will supersede all other policy areas which might be relevant.

To improve pupils' understanding and confidence in the procedures, it should be explained to all pupils what will happen when they report an incident or concern. This will improve pupil confidence and assure them that they are doing the right thing in reporting, and result in an increased likelihood of genuine reports being made if the pupils believe they are likely to be taken seriously.

Is the content illegal?

If the content involves an indecent image of a child on a website, a pupil can report the content using the CEOP button. The CEOP button can be found on the CEOP website, and leads to this report form: https://www.ceop.police.uk/Ceop-Report/. The CEOP report system is fairly child friendly.

A member of staff might also want to report via the IWF website. The Internet Watch Foundation provides a reporting system for illegal images and obscene content. The IWF report form location is here: https://www.iwf.org.uk/report

The IWF form should be used to report:
*   Child sexual abuse images hosted anywhere in the world
*   Non-photographic child sexual abuse images hosted in the UK
*   Criminally obscene adult content hosted in the UK

The IWF form is not child friendly, although secondary school pupils should be able to navigate it. Pupils should be encouraged to use the CEOP report form, which is child friendly. If a pupil reports an indecent or illegal image or content to a member of staff, the member of staff should help the child use the CEOP form, and might also consider the IWF form.

If a child reports an indecent image via CEOP the images will be investigated by SOCA (Serious Organised Crime Agency) of which CEOP is a department. CEOP's role is to work in partnership with government, the police service, child protection agencies, childrens' charities and industry to protect children, young people, families and society from paedophiles and sex offenders, in particular those who use the internet and other new technologies in the sexual exploitation of children.
*   CEOP often use the same agencies as the IWF to remove the images from the internet, by contacting ISPs and hosting providers.
*   The IWF will contact CEOP/SOCA with regard to reporting the criminal aspect of the material.

Reporting an image to IWF will result in the image being removed from the internet more quickly. Reporting an image to CEOP will result in the crime being logged more quickly. There is no reason not to report to both, although it is advisable to state this when reporting.

If the pupil wants to report other illegal content, such as grooming, sexting, threats, blackmail, or inappropriate contact from an adult or stranger – whether it involves themselves or a friend – they should be taught and encouraged to use the CEOP button.

School website administrators should include a button linking to the CEOP report page on the school website. The CEOP button should be placed (via an embed code) onto the school website, and internet school network pages. It's also worth placing the report button onto secure pupil email login portals and extranets.
*   Buttons and scripts for website administrators can be obtained here: https://www.thinkuknow.co.uk/AssetsLibrary/ or by contacting CEOP.
*   It is also possible to add a CEOP website add-on to every computer browser in school. Browser safety tools can be found here: https://www.thinkuknow.co.uk/parents/browser-safety/

It is important to note that indecent or illegal images should not be recorded or copied onto staff computers or school management systems as part of a school investigation. Copying an indecent image is a criminal offence which could result in an allegation made against a teacher, and a prosecution. Any images should be reported as a url link via the CEOP website. If the images or content is stored on a device, such as a laptop, mobile phone or computer, the computer should be disconnected from the network and securely stored. If in any doubt, CEOP / police advice should be sought first.

Depending on the specifics of the incident, the E-Safety Officer, Child Protection Officer or Head Teacher might need to liaise with local police, other agencies and if there is a child protection issue, the LADO. It is also worth considering Informing parents/carers, updating and evaluating risk assessments, determining appropriate counselling and considering pupil discipline in line with the schools e-safety / ICT acceptable use policy and behaviour policy.

Is the content inappropriate, but not illegal?

If the pupil wishes to report something which is inappropriate, but not illegal, such as adult pornography, copyright infringement, cyberbullying, harassment or offensive comments, then pupils should be taught and encouraged to use an online form added to the school's website, intranet, networked computers, webmail logins and extranets. It is worth allowing both named and anonymous usage of this form – although using a name should be encouraged.

- Here is an example of such a form: http://www.berkswellschool.org.uk/content.php?pageid=55

For any online reporting procedure, there should be an equivalent offline reporting procedure. Normally this will involve telling a member of staff at school. However, schools might consider using anonymous bullying reporting procedures, comments boxes or an in-tray for named e-safety reports written onto a pro-forma, or a weekly e-safety/bullying informal forum or circle time to cover and evidence the reporting of e-safety events.

- An example of coding for a school website bullying report form can be seen here: https://tuairisc.me/. This concept is adaptable for e-safety use.

Have school ICT systems been abused?

When pupils report an e-safety incident which involves the misuse of school IT facilities, it is highly likely the pupil/school acceptable use agreement will have been broken. All affected pupils, as part of pastoral care and behaviour management, will need to have the rules, behaviours and expectations contained in the AUP reiterated, and the consequences of any breach in the rules explained. It is always worth relating breaches in standards of acceptable behaviour in school to relevant situations in adult life, and how this can affect job prospects and a person's digital footprint.

Is cyber bullying or harassment involved?

Pupils should be encouraged – in addition to reporting to school staff – to report to Childline for issues such as bullying, self-harm, cyber bullying, childrens' rights, and child protection concerns which they are not comfortable sharing at school. Childline can be contacted at http://www.childline.org.uk or 0800 1111.

Cybermentors - http://www.cybermentors.org.uk/ can offer pupils informal and anonymous advice regarding cyber bullying or online behaviour which makes them feel uncomfortable.

Other advice:

It is worth feeder primary schools liaising with the local secondary school to standardise reporting procedures and the style of feedback pupils can expect.

Reporting procedures need to be reviewed regularly. The internet, and pupil usage of the internet, can change rapidly over a short period of time. A procedure which works now may well not encompass the needs and concerns of pupils in six months time. The e-safety coordinator needs to monitor current trends, but also talk to pupils regularly and elicit current trends within the particular school. School councils and informal forums are useful to monitor and evidence this.

Documenting how reporting procedures are informed by current trends also needs to be fed into staff inset and support staff training for e-safety. This will help the school stay ahead of the game, especially when considering liaising with relevant agencies or involving counselling services.