Berwick Academy Policy on E Safety

Overview

The purpose of this document is to describe the rules and guidance associated with E Safety and the procedures to be followed in the event of an E Safety incident at Berwick Academy.

Scope

This Policy applies to all students and staff, or any other person who utilises ICT communication and internet provision at Berwick Academy

The Policy covers the safe use and security requirements and safeguarding functions that are in place in order to protect students and staff.

The Policy should be read in conjunction with Academy's ICT Information Security Policy. This document can be found on the network or from the ICT Manager.

1. See also policies on;

Bullying
Child protection
Equal Opportunities
ICT Network Security
Bring Your Own Device (BYOD)
Recruitment
Safeguarding
Health and Safety
Use of Force

2. Role of E Safety Officer

- The E Safety Officer – Eddie Jefferson
- The following points outline the key aspects of the E Safety Officer's role within Berwick Academy.
  - Act as a single point of contact for all E Safety issues.
  - Liaise with national and international agencies such as the Child Exploitation and Online Protection Centre (CEOP).
  - Develop policy and practice for E Safety.
  - Be aware of potential risks from new and emerging technologies and, if appropriate, communicate these to staff and students.
  - Provide information, training and resources.
  - Regularly produce E-Safety reports via the e-safety monitoring system, Securus.
  - Report any E-Safety related incidents, deemed serious, to the Pastoral Head.

3. Why the internet and digital communications are important

- The internet is an essential element in 21st century life for education, business and social interaction.
  The school has a duty to provide students with high-quality internet access as part of their learning experience.
- Internet use is part of the statutory curriculum and a necessary learning tool for staff and pupils.

4. Internet use will enhance and extend learning

- The school internet access is designed expressly for pupil use and includes filtering appropriate to the age of the pupils.
- Clear boundaries are set for the appropriate use of the internet and digital communications and discussed with staff and pupils.
- Pupils will be educated in the effective use of the internet for research, including the skills of knowledge location, retrieval and evaluation.

5. Pupils will be taught how to evaluate Internet content

- The school ensures that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

6. Managing Internet Access

- ICT system security will be reviewed regularly.
- Virus protection is installed and updated regularly.
- Software must not be installed on any school device. All installs are performed by ICT Technical staff.
- All USB storage devices are not permitted to be used on the school network. Windows Group Policy Objects are in place for this purpose.

7. E-mail

- Students may only use school provided e-mail accounts on the school system.
- Students must immediately tell a teacher if they receive offensive e-mail.
- In e-mail communication, students must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Students and staff must take into account the sensitivity of any data, message or other communication before sending any e-mail.
- Staff e-mail facilities are provided primarily for school business use however; it is acknowledged that in some exceptional circumstances it may be permissible to respond to a private e-mail. Regardless of this, school e-mail facilities must never be used in connection with any secondary business activities.
- User mail boxes and their contents may be examined by the school, the LEA, its auditors or any law enforcement agency. Due consideration of the provisions of the

Human Rights Act and any other legislation will be made when undertaking such examinations.

- Any improper use of internal or external e-mail, as defined in this policy, or otherwise, may be considered by the school to be a disciplinary matter.
- The school prohibits the use of e-mail for purposes which may be illegal or the making or sending of e-mail messages which may be considered to be offensive in any way.
- E-mail must not be used :
  - To make possibly defamatory statements about any person or corporate body.
  - For sexual, racial or other harassment of any person.
  - To incite radicalisation and extremism in any form.

8. Published content and the school web site

- Staff or student personal contact information will not generally be published. The contact details given online are for the school office.

9. Publishing Pupil's Images and Work

- Pupils' full names will not be used anywhere on the school website or other online space, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- Work can only be published with the permission of the pupil and the parents/carers.
- Pupil image file names will not refer to the pupil by name.

10. Social networking, personal publishing and mobile phones

- The school will control access to social networking sites, and consider how to educate students in their safe use.
- Newsgroups will be blocked unless a specific use is approved.
- Students will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Students will be advised not to place personal photos on any social network space without considering how the photo could be used now or in the future.
- Staff members using social networking sites should ensure that all appropriate security settings are in place.
- Under no circumstances should staff members communicate with students via social networking sites.
- Staff will be advised not to use personal mobile phones to communicate with pupils.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

11. Managing filtering

- The school will work in partnership with the Internet Service Provider to ensure that systems to protect pupils are reviewed and improved.

- If staff or students discover an unsuitable site, it must be reported to the E Safety Officer.
- Securus web monitoring software is used in school to monitor the internet and general PC usage of all students and staff. All school computers, including laptops, which leave the school premises, has the Securus monitoring software installed. Internet usage is monitored for policy and legislative compliance. For further information refer to the "Monitoring of Internet Usage" section of the Berwick Academy Network Security Policy.
- We use two layers of filtering. Smoothwall Unified Threat Management (UTM) and Securus E-Safety Education. The filtering works by applying categories that should be blocked, e.g. Legal and Liability Issues, Adult Themes, Business and Corporate, Entertainment, File and Image Hosting, File Types, Finance, Information and Reference, IT and Technical, Lifestyle, Malware and Hacking, Medical, Multimedia, Search Engines, Social Media and Web Infrastructure.
- Recent emergence of Radicalisation and Extremism has necessitated the filtering of such content and this Sub-Category sits beneath the parent category of Adult Themes.

12. Managing videoconferencing (if used)

- IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- Students should ask permission from the supervising teacher before making or answering a videoconferencing call.
- Videoconferencing will be appropriately supervised for the students' age.

13. Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulation 2018.
- Personal data will be processed fairly and lawfully and will be obtained only for specified and lawful purposes. The information will be adequate, relevant and not excessive for its purpose. The information will be kept accurate and up to date. It will be kept for longer than is necessary and will be retained securely.

14. Code of Confidentiality

- Where appropriate and lawful, the sharing of information with a third party will be subject to and compliant with a Confidentiality Agreement signed by all parties.

15. Physical Security

- ICT equipment/paper/tapes/disks etc are disposed of in a controlled manner. Further information can be seen in sections 30, 31, 32 of the Berwick Academy ICT Network Security Policy.

16. Logical Access Controls

- All teaching staff and pupils use individual user IDs and passwords. The requirements set on the user accounts are as follows:
- Passwords must contain a minimum of 7 characters.
- Passwords must be alpha-numeric and contain at least 1 digit.
- Passwords must be changed every 90 days.
- Passwords cannot be reused within 20 password changes.
- If staff or students fail to login in 5 attempts the user account will be locked.
- Staff and students log out when finished using computers and should not leave logged in terminals unattended.

17. Policy Decisions

- **Authorising Internet Access**

    - All staff must read and sign the 'Code of Conduct for ICT' before using any school ICT resource.
    - The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
    - Students must apply for internet access individually by agreeing to comply with the Internet Use Statement.
    - Parents/Carers will be asked to sign and return a consent form.

18. 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 nor Northumberland County Council can accept liability for any material accessed, or any consequences of Internet access.
- The school will audit ICT use to establish if the E Safety policy is adequate and that the implementation of the E Safety policy is appropriate and effective.

19. Handling E Safety complaints

- Complaints of Internet misuse will be dealt with by the E-Safety Officer.
- Any complaint about staff misuse must be referred to the head teacher.
- Staff should report cases of deliberate inappropriate internet access by following the procedures in appendix A
- Staff should report cases of accidental inappropriate internet access by following the procedures in appendix B
- The Northumberland County Council recommended procedures for reporting incidents are outlined in appendix C.

20. Communicating E Safety

- **Introducing the E Safety policy to pupils**

    - E Safety rules will be posted in all rooms where computers are used.

- Students will be informed that network and internet use will be monitored.
- A programme of training in E Safety will be developed, based on the materials from CEOP.
- Online training is made available via the school subscription to E-Safety-Support.

- **Staff and the E Safety policy**

  - All staff will be given the School E Safety policy and its importance explained.
  - Staff will be informed that network and internet traffic can be monitored and traced to the individual user.
  - Staff should understand that phone or online communications with pupils can lead to misunderstandings or even malicious accusations. Staff must take care always to maintain a professional relationship.
  - Members of staff must not to use personal mobile phones to communicate with pupils and parents.
  - Members of staff must not communicate with students via social networking sites.

21. Enlisting parents' and carers' support

- Parents' and carer's attention will be drawn to the school E Safety policy in newsletters, the school brochure and on the school web site.
- The school will maintain a list of E Safety resources for parents/carers on the Web site.

22 Bring Your Own Device (BYOD)

- Students and Parents must read and sign the BYOD Policy before accessing the BYOD wireless network.

- Internet access is filtered by the school Smoothwall filtering system.

- The BYOD network is on a segmented, separate network to the school admin and curriculum networks. BYOD devices can only access the internet. Internal resources are accessed via the Magellan web portal.

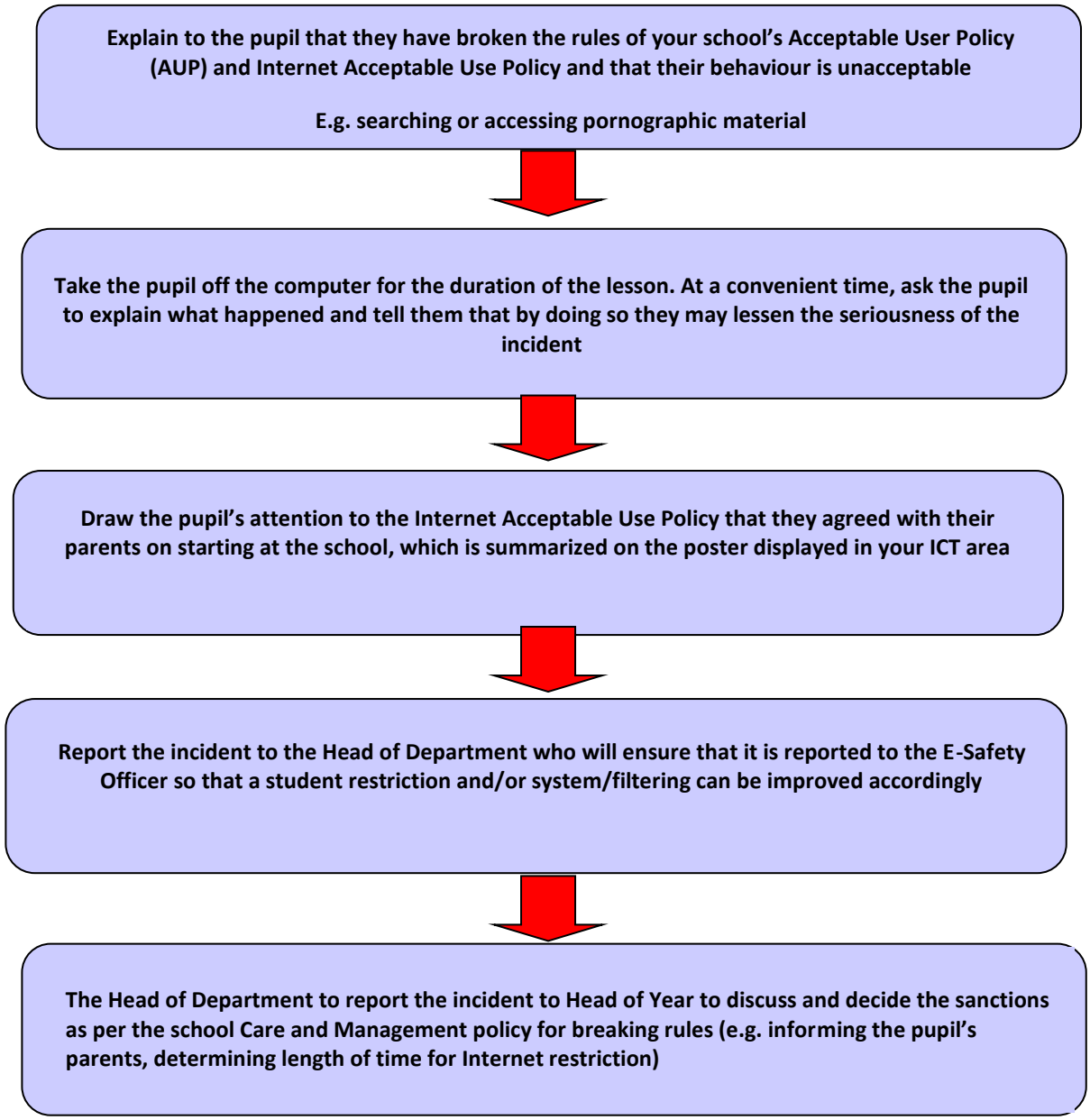
- Use is monitored via the AeroHive Cloud Management Portal.

Appendix A

Deliberate Inappropriate Internet Access

Whilst using the Internet during school hours, a pupil **deliberately** breaches the **Internet Acceptable Use Policy**. What should you do?

Use this step-by-step guide to help you follow the correct procedure for dealing with pupils who **deliberately** breaches the **Internet Acceptable Use Policy.**

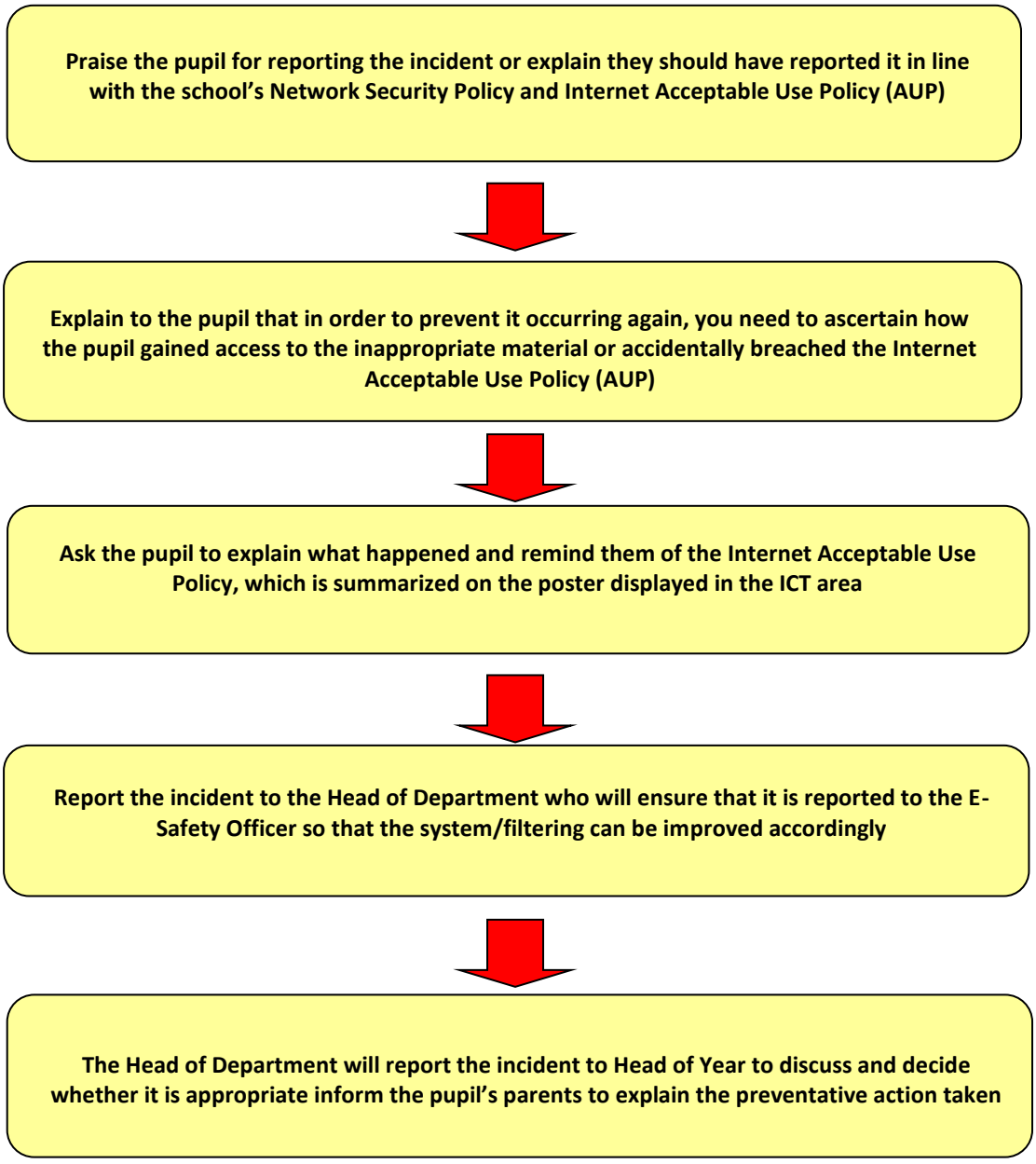


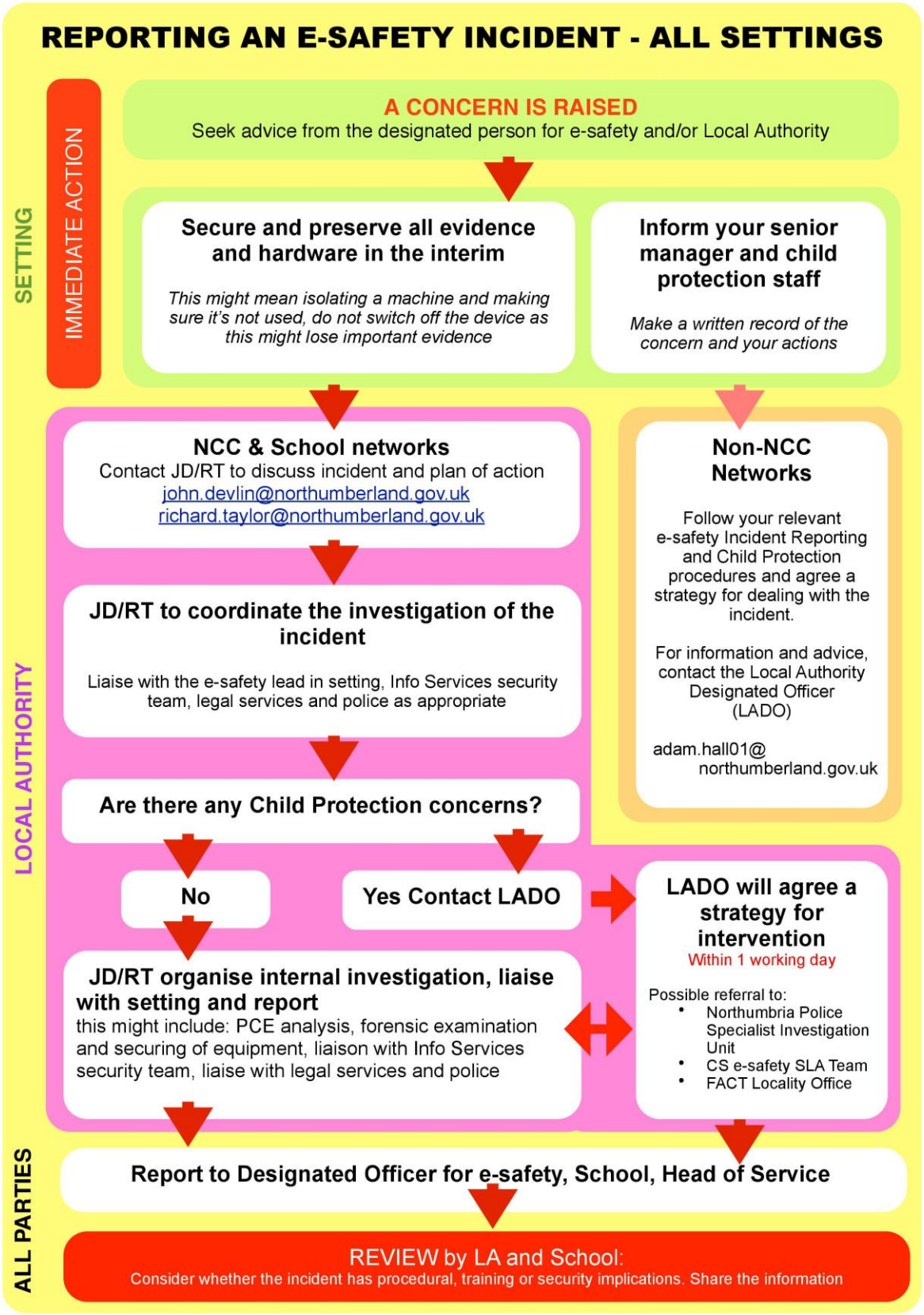
Appendix B

Accidental Inappropriate Internet Access

Whilst using the Internet during school hours, a pupil **accidentally** breaches the **Internet Acceptable Use Policy.** What should you do?

Use this step-by-step guide to help you follow the correct procedure for reporting a pupil who **accidentally** breaches the **Internet Acceptable Use Policy.**




REPORTING AN E-SAFETY INCIDENT - ALL SETTINGS
SETTING
IMMEDIATE ACTION
A CONCERN IS RAISED
Seek advice from the designated person for e-safety and/or Local Authority
Secure and preserve all evidence and hardware in the interim
This might mean isolating a machine and making sure it's not used, do not switch off the device as this might lose important evidence
Inform your senior manager and child protection staff
Make a written record of the concern and your actions
LOCAL AUTHORITY
NCC & School networks
Contact JD/RT to discuss incident and plan of action
john.devlin@northumberland.gov.uk
richard.taylor@northumberland.gov.uk
Non-NCC Networks
Follow your relevant e-safety Incident Reporting and Child Protection procedures and agree a strategy for dealing with the incident.
For information and advice, contact the Local Authority Designated Officer (LADO)
adam.hall01@northumberland.gov.uk
JD/RT to coordinate the investigation of the incident
Liaise with the e-safety lead in setting, Info Services security team, legal services and police as appropriate
Are there any Child Protection concerns?
No
Yes Contact LADO
LADO will agree a strategy for intervention
Within 1 working day
Possible referral to:
Northumbria Police Specialist Investigation Unit
CS e-safety SLA Team
FACT Locality Office
JD/RT organise internal investigation, liaise with setting and report
this might include: PCE analysis, forensic examination and securing of equipment, liaison with Info Services security team, liaise with legal services and police
ALL PARTIES
Report to Designated Officer for e-safety, School, Head of Service
REVIEW by LA and School:
Consider whether the incident has procedural, training or security implications. Share the information

Version History

Record of issued versions				
Author	**Approved date**	**Committee**	**Version**	**Status**
Eddie Jefferson	09/11/2010	Full Governing Body	1.0	Final Version
Eddie Jefferson	14/04/2010	Full Governing Body	2.0	Social networking section added.
Eddie Jefferson	18/08/2012	Full Governing Body	3.0	Amended due to the change to academy status
Eddie Jefferson	25/06/2014	Full Governing Body	4.0	Reviewed
Eddie Jefferson	14/10/2015	FGPC	5.0	Amended due to the emergence of Radicalisation and Extremism in UK
Eddie Jefferson	11/10/2017 25/05/2018	FGPC	6.0 6.1	Amended due to BYOD being added to 6th form Reference to Data Protection updated to GDPR 2018
Eddie Jefferson	12/02/2020	Full Trustee Board	6.2	6) USB storage devices are not permitted on the school network. 7) Students should only use school email accounts that are assigned to them. 20) Online E-Safety training is provided. Appendix B Changed NCC reporting flowchart so new

				LADO contact details are displayed