EXCELSIOR ACADEMY

E-Safety Policy

E-Safety Policy

Introduction

Excelsior Academy firmly believes that the effective use of information and communication technologies in the academy can bring great benefits. Recognising the e-safety issues and planning accordingly will help to ensure appropriate, effective and safer use of digital technologies.

This e-safety policy has been developed by a working group made up of:

- School E-Safety Co-ordinator
- Principal
- Strategy Manager for Pupil Welfare
- ICT Technical Manager

Consultation with the whole academy has taken place through

- School Council
- Staff meetings

Scope of the Policy

This policy applies to all members of the academy community (staff, pupils, volunteers, parents / carers, visitors and community users and other individuals who work for or provide services on behalf of Excelsior Academy) who have access to and are users of the school ICT systems both in and out of school.

The Education and Inspections Act empowers Headteachers / School Principals, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber bullying or other e-safety incidents covered in this policy, which may take place out of school, but is linked to membership of the academy.

The academy will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that will take place inside and outside of the academy.

This policy covers personal use of social media as well as the use of social media for official school purposes, including sites hosted and maintained on behalf of Excelsior Academy.

This policy applies to personal webspace such as social networking sites (for example Facebook), blogs, microblogs such as Twitter, chatrooms, forums podcasts, open access online encyclopaedias such as Wikipedia, social bookmarking sites such as del.icio.us and content sharing sites such as flickr and YouTube. The internet is a fast moving technology and it is impossible to cover all circumstances or emerging media – the principles set out in this policy must be followed irrespective of the medium.

Context

We live in a digital age where technology is playing an ever increasing part of our lives; it is changing the way that we do things both inside and outside of school and although we recognise the benefits of technology we must also be aware of the potential risks and ensure that all staff, pupils and parents / carers associated with the academy are to use technology in a safe and responsible manner.

Some of the potential dangers of using technology may include:

- Inappropriate use of social media
- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- Inappropriate communication / contact with others including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person

Many of these risks reflect situations in the online world but it is important that as an Academy we have a planned and coordinated approach to ensuring that all involved with the academy use technology in a safe and responsible way. As with all risks it is impossible to eliminate them completely but with a planned and coordinated approach they can be significantly reduced and users can be taught to manage them effectively.

Social Media

Background

Social media is now an everyday part of modern life. Communicating online with friends, colleagues and people you've never even met is commonplace thanks to the rapid rise of platforms such as Facebook and Twitter.

Excelsior Academy recognises the major benefits social media has brought in its communication with pupils, parents, the local community and media.

Excelsior has embraced social media, creating its own Facebook, Twitter, Tumbler and YouTube accounts, gaining hundreds of friends and followers as a result. The academy's social media accounts are assisting pupil learning and development.

The academy has much to celebrate and share with its audiences and will continue to adopt the latest technology to do this. But communication through social media has to be balanced with our duties as a school, our legal responsibilities and guarding our reputation.

Excelsior sets out guidelines in this document about what is and what is not acceptable behaviour by academy staff on social media platforms, both personal and school sanctioned accounts.

This document aims to balance our continued support of innovative communication with good practice requirements.

The purpose of the guidelines are to:

- Safeguard all school pupils
- Encourage a consistent approach to the adoption, maintenance and monitoring of social media.
- Inform staff of acceptable and unacceptable behaviour on personal and Excelsior sanctioned social media sites

- Protect the academy from legal risks
- Ensure that the reputation of Excelsior, its staff and governors is protected

Definition of Social Media

Websites and applications that enable users to create and share content or participate in social networking.

Examples include Twitter, Facebook, Pinterest, YouTube, Flickr, Tumblr, Google + and Linkedin and comment streams on websites such as newspaper sites.

All members of staff should be aware that information they share through social networking sites is subject to legal scrutiny, such as defamation copyright, data protection and Freedom of Information legislation.

The open nature of the internet means that social networking sites can leave members of staff vulnerable if they fail to observe a few simple precautions.

Legal Framework

Excelsior Academy is committed to ensuring that all staff members provide confidential services that meet the highest standards. All individuals working on behalf of Excelsior Academy are bound by a legal duty of confidence and other laws to protect the confidential information they have access to during the course of their work.

Disclosure of confidential information on social media is likely to be a breach of a number of laws and professional codes of conduct, including:

- The Human Rights Act 1998
- Common law duty of confidentiality
- The Data Protection Act 1998.

Confidential information includes, but is not limited to:

- Person-identifiable information, e.g. pupil/student and employee records protected by the Data Protection Act 1998
- Information divulged in the expectation of confidentiality
- School business or corporate records containing organisationally or publicly sensitive information
- Any commercially sensitive information such as information relating to commercial proposals or current negotiations
- Politically sensitive information

Staff members should also be aware that other laws relating to libel, defamation, harassment and copyright may apply to information posted on social media, including:

- Libel Act 1843
- Defamation Acts 1952 and 1996
- Protection from Harassment Act 1997
- Criminal Justice and Public Order Act 1994
- Malicious Communications Act 1998
- Communications Act 2003
- Copyright, Designs and Patents Act 1988

Excelsior Academy could be held vicariously responsible for acts of their employees in the course of their employment. For example, staff members who harass co-workings online or who engage in cyberbullying or discrimination on the grounds of race, sex, disability, etc or who defame a third party while at work may render Excelsior Academy liable to the injured party.

Personal Use of Social Media

School staff will not invite, accept or engage in any social media communication with pupils/students at Excelsior Academy, their parents or their guardians.

Excelsior Academy does not expect staff members to discontinue contact with their family members via personal social media once the school starts providing services for them. However, any information staff members obtain in the course of their employment must not be used for personal gain nor be passed on to others who may use it in such a way.

If staff members wish to communicate with pupils/students through social media sites or to enable pupils/students to keep in touch with one another, they can only do so with the approval of the Academy and through official Excelsior Academy sites created according to the requirements set out below in paragraph: -

Excelsior Academy sanctioned use of social media

Staff members must decline 'friend requests' from pupils/students they receive in their personal social media accounts. Any communication received from an academy pupil on a personal social media site must be reported to the reporting member of staffs' school Principal/line manager.

Members of Excelsior staff are strongly advised to set all privacy settings to the highest possible levels on all personal social media accounts. Staff should make clear on personal social media accounts that they are expressing their own views.

Staff members should keep their passwords confidential, change them often and protect their social media passwords and account details to avoid unauthorised use – particularly where one touch access might give open access via an app on a phone or tablet. Any device used for Excelsior Academy social media accounts must be password protected or be used with a lock code in place.

Think before you tweet – staff should avoid posts or making comment on specific matters related to the academy. Staff are advised to consider the reputation of Excelsior Academy in any posts they make relating to the academy. No posts should be made which could in any way damage Excelsior Academy's reputation.

On leaving Excelsior Academy's service, staff members must not contact Excelsior Academy pupils/students by means of personal social media sites.

Information staff members have access to as part of their employment, including personal information about pupils/students and their family members, colleagues, and other parties and school corporate information must not be discussed on their personal social media accounts.

Photographs, videos or any other types of image of pupils/students and their families or images depicting staff members wearing clothing with school logos or images identifying sensitive school premises must not be published on personal webspace.

Excelsior Academy email addresses and other official contact details must not be used for setting up personal social media accounts or to communicate through such media.

Staff members must not edit open access online encyclopaedias such as Wikipedia in a personal capacity at work. This is because the source of the correction will be recorded as the employer's IP address and the intervention will, therefore, appear as if it comes from the employer itself.

The Excelsior Academy corporate logos or brands must not be used or published on personal webspace.

Excelsior Academy Sanctioned Use of Social Media

Staff setting up social media accounts or sites for educational purposes in Excelsior Academy's name must first consult and gain approval from Dawn Charlton, Excelsior's Business Manager.

Excelsior sanctioned accounts will strictly be created for educational purposes and should be entirely separate to personal accounts. They should ideally provide a link to an academy email account.

The content of Excelsior sanctioned accounts must be professional and reflect well on the academy. Staff must not publish photographs or names of children on Excelsior sanctioned accounts without the written consent of parents or guardians.

Staff should ensure when posting links to content that the content is appropriate and safe for viewing.

Any abuse or inappropriate comments on Excelsior sanctioned accounts should be removed and reported to the academy communications and publicity manager.

No direct messaging should take place between staff and pupils through Excelsior social media accounts.

Staff members must at all times act in the best interests of children and young people when creating, participating in or contributing content to social media sites.

The Use of Digital Images and Videos

The development of digital imaging technologies has created significant benefits to learning, allowing school staff and pupils instant use of images they have recorded themselves or downloaded from the internet. School staff and pupils are made aware of the potential risks associated with storing, sharing and posting images on the internet and must follow the good practice detailed below.

- When using digital images, staff will inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they will recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Staffs are permitted to take digital images and videos to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purpose.
- Care will be taken when capturing digital images and videos that pupils that are appropriately dressed and are not participating in activities that might bring individuals or the school into disrepute.

- Pupils must not take, use, share, publish or distribute images of others without their permission
- Images and videos published on the school website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils full names will not be used anywhere on a website or blog, particularly in association with photographs
- Written permission from parents and carers will be obtained before photographs of pupils are published on the school website.
- Pupils work will only be published with the permission of the pupil and parents or carers.

Breaches of the Policy

Any breach of this policy may lead to disciplinary action being taken against the staff member/s involved in line with Excelsior Academy's Disciplinary Policy.

A breach of this policy leading to breaches of confidentiality or defamation or damage to the reputation of Excelsior Academy or any illegal acts or acts that render Excelsior Academy liable to third parties may result in disciplinary action or dismissal.

Data Security and Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than necessary
- Processed in accordance with the data subject rights
- Secure
- Only transferred to others with adequate protection

All academy staff will ensure that:

- Care is taken to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- Personal data is used or processed on only secure password protected computers and other devices and that these devices are properly 'logged off' at the end of any session in which they are using personal data
- Data is transferred securely using encryption and secure password protected devices and email solutions.
- When personal data is stored on any portable computer system, USB stick or any other removable media:
    - The data must be encrypted and password protected
    - The device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected)
    - The device must offer approved virus and malware checking software
    - The data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use complete

Pupil Acceptable Use Policy (AUP) points:

Item	Category	Some examples of misuse
Use of Trust systems and services is a privilege. Individuals may be prevented from using the systems or services if they present a risk to the system, themselves or others.	Access and Security	Breach of any of the above.
Data will normally be saved to a network drive – an individual's Documents / H: Drive or the Learning Space.	Data	Data will normally be saved to an Academy network drive, an individual's Documents / H: Drive or the VLE.
Where data has been inadvertently overwritten or removed from the system, IT Support must be notified immediately, via a Teacher, to give the greatest chance of recovering the data.	Data	Realising a file has been overwritten or removed but not reporting it for weeks.
E-mail access is provided to benefit your studies at Excelsior Academy	Use of E-mail	Using Academy e-mail for frivolous purposes.
E-mail is only to be used for Excelsior Academy purposes.	Use of E-mail	Using Academy e-mail for frivolous purposes.
Only e-mail those you know, or are required to communicate with as part of your studies at Excelsior Academy.	Use of E-mail	E-mailing unknown persons.
Do not send e-mails containing offensive language or content.	Use of E-mail	Including profanities or derogatory e-mails.
Report e-mails from senders you do not recognise, inappropriate e-mails you receive, suspected misuse or bullying to your school's Welfare Manager.	Use of E-mail	Not reporting inappropriate e-mails, misuse or bullying.
Misuse of e-mail will be referred to the Behaviour Teams.	Use of E-mail	Breach of any of the above.
It is forbidden to give your address, telephone number or any other contact details, or those of others, or to arrange to meet someone unless your parent, carer or teacher has given permission.	Use of E-mail	Giving out personal information.
Some pages are blocked by the Trust web filter. Should a page be required for your schools work a request should be submitted to IT Support via a member of staff.	Use of the Internet	Use of proxy websites to get to blocked pages.
Equipment must be checked for damage or faults prior to use. Any damage or faults must be reported to IT Support via a member of staff	General use	Failure to report damage or faults to a member of staff.

Any inappropriate use or content be identified will be referred to the Behaviour staff.	General notices	

Staff AUP points:

Item	Category	Some examples of misuse
Trust systems and services must only be accessed by authorised individuals using their own username and password.	Access and Security	Use of another person's account.
Passwords, user accounts and access codes must be kept securely and never given to others, including IT Service personnel, without permission in writing from the Business Manager.	Access and Security	Writing down passwords, sharing passwords or an individual allowing others to use their user account.
Passwords must be at least 8 characters in length, include at least one uppercase letter, one lowercase letter, one number and one special character, must not be one of the last three passwords used and must be changed every 90 days.	Access and Security	Using simple passwords, e.g. 'Excelsior', '12345', 'qwerty' or that individual's name.
Devices must be locked or logged off when left unattended – even if a room is locked when left.	Access and Security	Leaving a computer unlocked and unattended.
Devices which automatically connect to Trust services, such as downloading e-mail, must only be accessed by the individual whose account is being used to automatically connect. I.e. family members or other persons may not use a Trust laptop, tablet or phone.	Access and Security	Use of an individual's account by another person.
It is the responsibility of each individual to keep their own user account, credentials and data safe.	Access and Security	Breach of any of the above.
Data will normally be saved to a network drive – an individual's Documents / H: Drive, Staff Resources, Pupil Resources or the Learning Space.	Data	Data will normally be saved to an Academy network drive, an individual's Documents / H: Drive or the VLE.
Where Trust data is not stored to the locations mentioned above it must be securely backed up to protect against equipment failure, theft or data corruption.	Data	Data stored away from Trust network and not backed up.
Additionally, where personal information is not stored on the locations mentioned in above the data must be encrypted and	Data	Personal information, e.g. names and photos, stored unencrypted away from the Trust network

password protected.		
Where data has been inadvertently overwritten or removed from the system, IT Support must be notified immediately to give the greatest chance of recovering the data.	Data	Realising a file has been overwritten or removed but not reporting it for weeks.
Each individual is responsible for ensuring the content of data they store on Trust equipment is appropriate and legal - and that the data has been lawfully obtained.	Data	Storage of inappropriate or illegal content on any Trust equipment.
Trust-provided e-mail may only be used for Trust business.	Use of E-mail	Using Academy e-mail for a personal financial gain or frivolous purposes.
Only open attachments or follow links in an e-mail if you recognise the sender and are expecting the attachment or link.	Use of E-mail	Opening an attachment or following a link from an unknown sender or from an e-mail which is not expected.
E-mail communication between staff and students may only be made using Trust provided E-mail accounts.	Use of E-mail	Use of personal e-mail accounts for staff to student or student to staff communication.
All web pages accessed must be appropriate, compatible with the interests of the Trust and legal.	Use of the Internet	Accessing a website which is not age appropriate or is illegal.
Should any inappropriate content be accessed by accident it must be immediately reported to the IT Service Manager.	Use of the Internet	Failure to report accidental access of inappropriate content.
Some pages are blocked by the Trust web filter. Should a page be required for Trust business a request should be submitted to IT Support	Use of the Internet	Use of proxy websites to get to blocked pages.
Use of proxy websites, or any other software or system, to circumvent the security of the Trust system and services is strictly forbidden.	General use	Use of proxy websites to get to blocked pages. Connecting a hotspot to the Academy network.
Equipment must be checked for damage or faults prior to use. Any damage or faults must be reported to IT Support by e-mailing helpdesk@excelsiornewcastle.org.uk.	General use	Failure to report damage or faults to IT Support.
Software or Hardware must not be installed or connected to any Trust owned device without permission in writing from the IT Service Manager.	General use	Installation of software without written permission from the IT Service Manager.
Trust computers may only be used for work which is compatible with the interests of the Trust.	General use	Use of Trust services or systems for illegal activities.

The Trust reserves the right to monitor all use of computer systems and services including e-mail, Internet access and use of computers.	General notices	
The Trust reserves the right to charge individuals for all costs relating to damages caused by them, through neglect or deliberate action, to Trust equipment or systems.	General notices	
Any inappropriate use or breaches of this policy will be referred to HR.	General notices	
Everyone has a responsibility to ensure they only access and store legal material on Trust computer Systems. Anyone who discovers of any illegal material or use of the computer systems must report it immediately to the Academy Executive Principal. Should any illegal use or content be confirmed it will be reported to the relevant authorities and dealt with through HR / behaviour teams.	General notices	

Digital Communication

Digital communication is an area that is developing rapidly with new and emerging technologies, devices are becoming more mobile and information sharing / communication is becoming more sophisticated.

When using communication technologies the academy ensures the following good practice:

- Pupils are not permitted to have mobile devices out of their pocket / bag during the academy day. Should a pupil need to take or make a call, the pupil should go to an office of a member of the Welfare Team. Mobile devices should be turned off during the school day
- The official school email service is regarding as safe and secure and is monitored. Staff and pupils should therefore only use the school email service to communicate with others when in school, on school business or on school systems.
- Users need to be aware that email communications may be monitored
- Users must immediately report the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any communication between staff, pupils or parents / carers (email, chat VLE, text etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes should not be used for these communications.
- Pupils will be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate communications via technologies and be reminded of the need to write such

communications clearly and correctly and not include any unsuitable or abusive material.
- Personal information will not be posted on the academy's website and only official email addresses should be used to identify members of staff

Unsuitable / Inappropriate Activities

School ICT systems are only to be used for agreed, appropriate and suitable work related activities. Internet activity which is considered unsuitable or inappropriate will not be allowed and if discovered will lead to disciplinary action. Internet activity which is illegak will be reported and could lead to criminal prosecution.

Responding to Incidents of Misuse

It is hoped that all members of the academy community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place accidently, through carless or irresponsible or, very rarely, through deliberate misuse.

In the event of an e-safety incident it is important that there is a considered, coordinated and consistent approach.

The Laidlaw Schools Trust ('the Trust') recognises that privately owned technology, e.g. mobile phones, tablet computers and laptops, provides an additional opportunity to use technology to benefit teaching and learning and Trust business operations. Whilst the use of Bring Your Own Device (BYOD) scheme presents opportunities it also brings risks, which must be carefully managed through technical solutions and policy. This document details how the Trust manages BYOD.

General Information

Any person accessing the Trust network, including on a private device or BYOD network, must comply with the Trust Acceptable Use Policy. Devices connected to the Trust network are subject to the same monitoring as Trust-owned devices.

Use of private devices

- Any individual bringing privately owned equipment to Trust/Academy premises is strongly advised to ensure the equipment is adequately insured to cover any damage or loss of equipment.
- All private devices must be patched with the latest available security updates and run anti-malware software with current definitions.

Staff

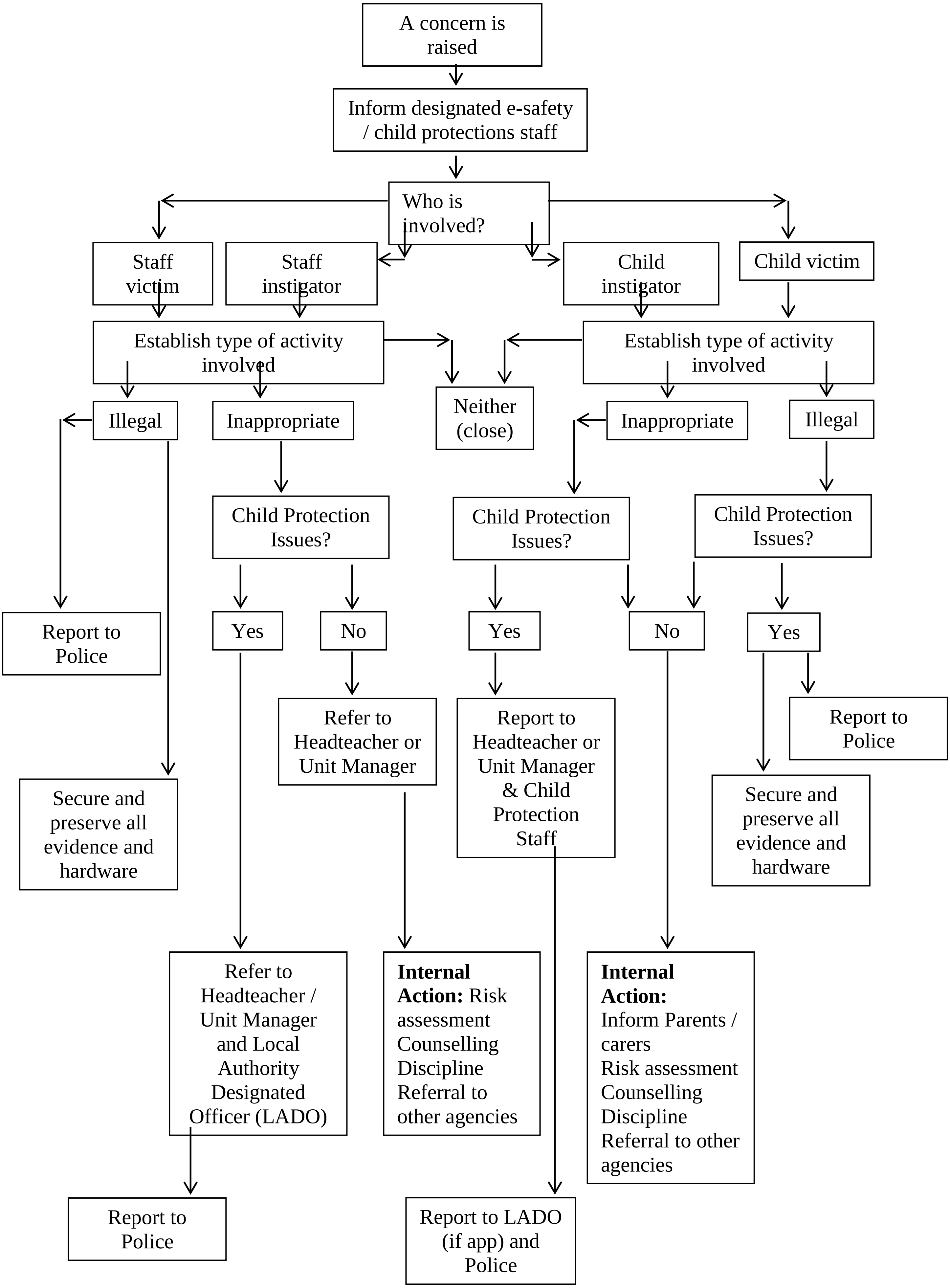
- Staff may wish, and are permitted, to access Academy or Trust e-mail on a private device – on or off the premises. Where this is done staff devices must enable a strong passcode (e.g. not one number repeated, 0000, 1234.) on the device to prevent Academy e-mails from being viewed. It is the individual's responsibility to set a secure passcode on a private device.
- Staff must never capture or store photographs, video recordings or other images of Academy pupils on private devices under any circumstances.
- If Trust/Academy data containing personal or sensitive information is stored on a private device, the device must be encrypted. It is the responsibility of the individual to ensure their device is encrypted.

Pupils

- Pupils are welcome to bring their own devices to Trust/Academy premises should they wish, but must follow direction of staff and behaviour policies regarding use.
- Photographs must never be taken of other pupils or staff (without their express permission).

Technical

- Private devices are connected to a network separate to the main Trust network which affords authenticated Internet and e-mail access only.


A concern is raised
Inform designated e-safety / child protections staff
Who is involved?
Staff victim
Staff instigator
Child instigator
Child victim
Establish type of activity involved
Neither (close)
Establish type of activity involved
Illegal
Inappropriate
Inappropriate
Illegal
Child Protection Issues?
Child Protection Issues?
Child Protection Issues?
Report to Police
Yes
No
Yes
No
Yes
Refer to Headteacher or Unit Manager
Report to Headteacher or Unit Manager & Child Protection Staff
Report to Police
Secure and preserve all evidence and hardware
Secure and preserve all evidence and hardware
Refer to Headteacher / Unit Manager and Local Authority Designated Officer (LADO)
Internal Action: Risk assessment Counselling Discipline Referral to other agencies
Internal Action: Inform Parents / carers Risk assessment Counselling Discipline Referral to other agencies
Report to Police
Report to LADO (if app) and Police