The Gryphon Trust

E-Safety Policy

GAT/0061

POLICIES AND PROCEDURES PROFORMA

Subject	E-Safety Policy
Version	1.0
Author	Miss Milligan, IT Manager
Persons / Committees consulted whilst document in draft	Headteachers Governing Body
Date Policy Agreed	March 2022
Date of Next Review and By Whom	September 2023 IT Manager
Copy obtainable from and / or distribution	PA to the Headteacher
Date Document Issued	September 2021
Responsibility for Dissemination to New Staff	Line Managers
Policy Review	Biennially
Headteacher Target Audience	All Staff All Students Parents Commissioning Schools Local Authorities

Amendments Summary:

Amend. No.	Issued	Page	Subject
1	March 2022		Policy review

E-Safety Policy

1.0 Scope of the Policy

1.1 This policy applies to all members of The Gryphon Trust community (staff, students, volunteers, parents/carers, visitors, and community users) who have access to and are usersof the Trust ICT systems, both in and out of school.

1.2 The Staff Code of Conduct (see the Gryphon Trust Manual of Personnel Practice) specifies acceptable ICT use criteria for all staff.

1.3 The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students when they are off the school sites 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 by this policy, which may take place out of school, but is linked to membership of the schools in the Trust.

1.4 The schools 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 take place inside and outside of Trust.

2.0 Context

2.1 We live in a digital age where technology is playing an ever-increasing part in our lives; it is changing the way that we do things both inside and outside of school.

2.2 The Gryphon Trust firmly believes that the effective use of information and communication technologies in schools can bring great benefits and although we recognise the benefits of technology we must also be aware of the potential risks and ensure that all staff, students and parents/carers associated with the school are able to use technology in a safe and responsible manner.

2.3 Some of the potential dangers of using technology may include:

- Access to illegal, harmful or inappropriate images or other content.
- Unauthorised access to/loss of/sharing of personal information.
- The risk of being subject to grooming by those with whom emotionallyvulnerable children make contact on the internet.
- The sharing/distribution of personal images without an individual’s consent orknowledge.
- Inappropriate communication/contact with others, including strangers.
- Cyber-bullying.
- Access to unsuitable video/internet games.
- An inability to evaluate the quality, accuracy and relevance of information onthe internet.
- Plagiarism and copyright infringement.
- Illegal downloading of music or video files.
- The potential for excessive use which may impact on the social and emotionaldevelopment and learning of the young person.

3.0 Infrastructure and Technology

3.1 The Gryphon Trust is responsible for ensuring that the school infrastructure/networks are as safe and secure as is reasonably possible.

3.2 The Trust's educational network and access to the internet is provided by Virgin. This network provides a safe and secure 200Mbps broadband connection to the internet at Eaglewood School and 500Mbps at The Arnewood School.

3.3 There is a multi-layer security shield that provides dual-layer firewall protection, intruderdetection/prevention, load balancing, content caching, data traffic analysis and virus protection. There is a cloud-based filtering service, which filters internet content which undertakes live scanning of all sites and blocks any threats or inappropriate websites.

3.4 The infrastructure has been designed to minimise the risk of; users accessing inappropriate material, data being lost or accessed by unauthorised users, virus or malware threats. All internet and network activity is logged and can be retrieved if required in the event of an investigation.

4.0 Education and Training

4.1 The Gryphon Trust is committed to ensuring that staff receive regular training to keepup to date with new developments and ensure that they are sufficiently confident to educate students in the safe and responsible use of technology.

4.2 The Gryphon Trust have designed an E-safety curriculum that meets the needs of all its students and ensures their safety and well-being. The curriculum is reviewed and revised on a regular basis to ensure that it remains current.

4.3 The Trust will also provide information and training opportunities for parents and carers and endeavour to raise their awareness of the technologies that their children are potentially using and the risks that they potentially face.

5.0 Policy Statements

5.1 The Trust will ensure that all access to the internet and ICT systems by students iseffectively managed and supervised.

5.2 As part of the E-safety policy the Trust will also manage:

- The use of digital images and video.
- Data protection.
- Digital communications.
- Unsuitable/inappropriate activities.
- Incidents of misuse.

6.0 The Use of Digital Images and Videos

6.1 The development of digital imaging technologies has created significant benefits to learning, allowing Trust staff and students instant use of images they have recordedthemselves or downloaded from the internet. The Gryphon Trust staff and students are made aware of the potential risks associated with storing, sharing, and posting images on the internet and must followthe good practice detailed below:

- Staff will inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they will recognisethe risks attached to publishing their own images on the internet e.g., on social networking sites.
- Staff are permitted to take digital images and video to support educational aims onTrust equipment alone and must follow school and Trust policies concerning the sharing, distribution, and publication of those images.
- Care will be taken when capturing digital images and video that students areappropriately dressed.
- Care will be taken when capturing digital images that students are not participatingin activities that might bring the individuals or the Trust into disrepute.
- Students must not take, use, share, publish or distribute images of others (studentsor staff) without their permission.
- Images and videos published on the Trust or school website, or elsewhere that include students will be selected carefully and will comply with good practice guidance onthe use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Permission from parents or carers and students will be obtained before photographs of students are published on the school website.

7.0 Data Security and Protection

7.1 The use by staff and monitoring by the Trust of its electronic communications systems is likely to involve the processing of personal data. Therefore, it is regulated by the UK General Data Protection Regulation (UK GDPR) and all data protection laws and guidance in force.

7.2 Personal data will also be recorded, processed, transferred and made available according to the Data Protection Act 2018 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 is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

7.3 All Trust staff will ensure that:

- Care is taken to ensure the safe keeping of personal data, minimising the risk of itsloss 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 anysession in which they are using personal data.
- Data is transferred securely using encryption and secure password protected devicesand email solutions.
- When personal data is stored on any portable computer system, USB stick or anyother removable media:

    - the data must be encrypted and password protected.
    - the device must offer approved virus and malware checking software.

- the data must be securely deleted from the device, in line with Trust policy(below) once it has been transferred or its use is complete.

8.0 Digital Communication

8.1 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 Trust ensuresthe following good practice:

- The official Trust email service is regarded as safe and secure and is monitored.
- Staff and students should only use the Trust email service to communicate with others when in the Trust schools, on Trust business or on Trust systems. Personal emails and devices must not be used for Trust communication.
- Any digital communication between staff, students or parents/carer must beprofessional in tone and content.
- 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 respondto any such email.
- Students will be taught about email safety issues, such as the risks attached to the use of personal details. They will also be taught to write emails clearly and correctlyand not include any unsuitable or abusive material.
- Key stage 2 and above will be provided with individual Trust/school email addresses for educational use.

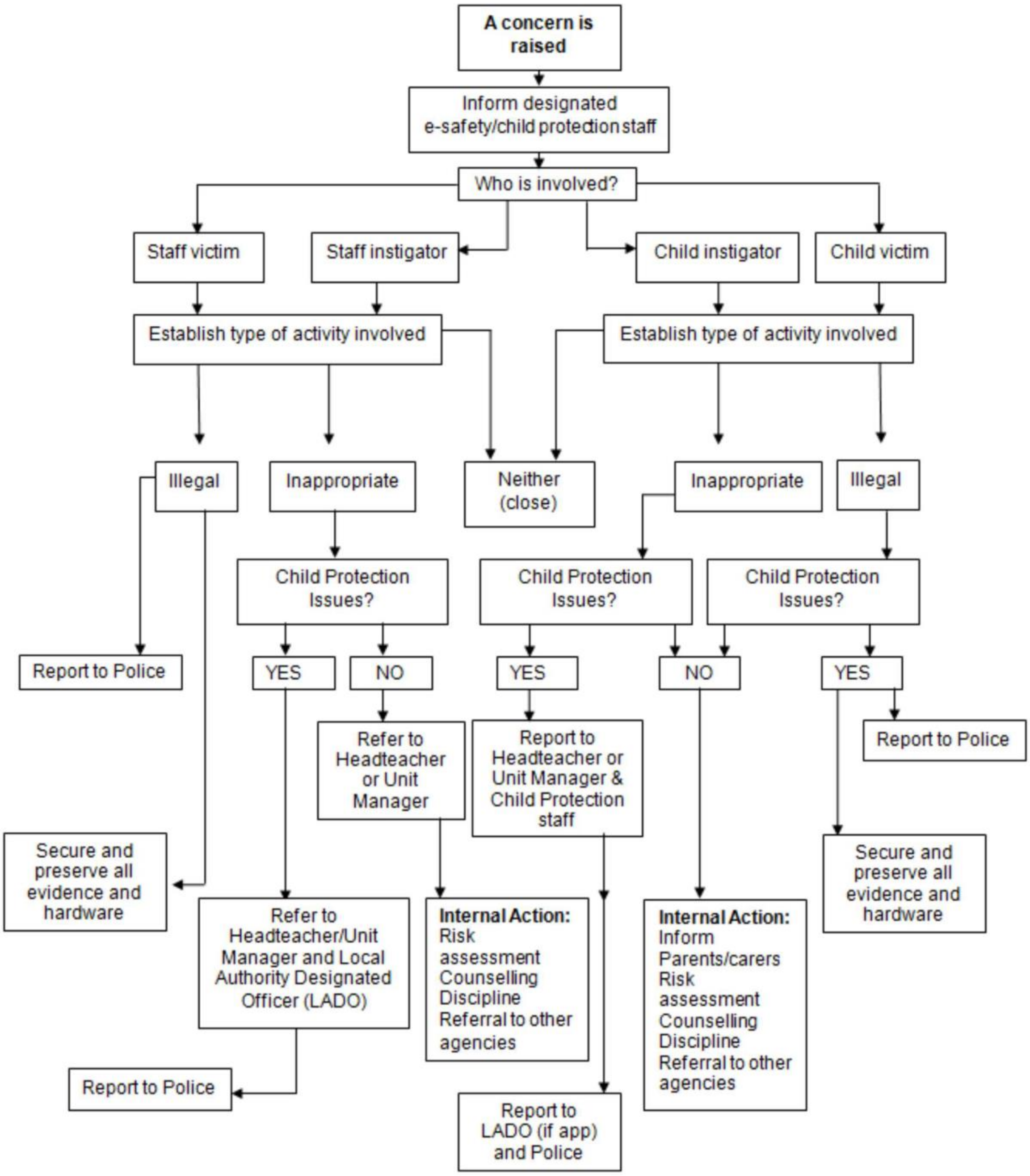
9.0 Unsuitable / Inappropriate Activities

9.1 Trust 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 illegal willbe reported and could lead to criminal prosecution.

10.0 Responding to Incidents of Misuse

10.1 It is hoped that all members of the Trust 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 careless or irresponsible or, very rarely, through deliberate misuse.

10.2 In the event of an e-safety incident it is important that there is a considered, coordinatedand consistent approach. Incidents will be managed using the incident flowchart below.


A concern is raised
Inform designated e-safety/child protection staff
Who is involved?
Staff victim
Staff instigator
Child instigator
Child victim
Establish type of activity involved
Establish type of activity involved
Illegal
Inappropriate
Neither (close)
Inappropriate
Illegal
Child Protection Issues?
Child Protection Issues?
Child Protection Issues?
Report to Police
YES
NO
YES
NO
YES
Report to Police
Refer to Headteacher or Unit Manager
Report to Headteacher or Unit Manager & Child Protection staff
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
Secure and preserve all evidence and hardware
Report to Police
Report to LADO (if app) and Police