The Wellington Academy

ROYAL WOOTTON BASSETT ACADEMY TRUST

E-SAFETY POLICY

This policy is applicable to all students, staff and parents of The Wellington Academy

DOCUMENT CONTROL	
Responsible position:	**Approved by:**
I.T. Director/DSL	Headteacher
Version number:	**Date approved:**
V 5.0	October 2020
Review Period:	**Next review date:**
Annually	October 2021

RELATED POLICIES AND DOCUMENTS
Policy Name
Safeguarding and Child Protection Policy
Freedom of Information Policy
Equal Opportunities Policy
Behaviour of Learning and Principles Policy
Health and Safety Policy
National Minimum Standards - Appendix 1/1; revision Sept 2014 Revised NMS

REVISION RECORD		
Date	**Version**	**Revision Description**
May 2013	1.0	Written in line with current legislation
June 2014	1.1	Updated for MAT
December 2014 May 2015	1.1	Reviewed for Boarding purposes
May 2018	1.2	Reviewed and updated
March	2.0	Reviewed and updated
April 2019	3.0	Reviewed and updated
October 2020	4.0	Reviewed and updated

INTRODUCTION

Safeguarding is a serious matter; we use technology and the internet extensively across all areas of the curriculum. Online safeguarding, known as e-safety, is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to changes in requirements or legislation, whichever is sooner.

The primary purpose of this policy is twofold:

- To ensure the whole Wellington community is provided with the knowledge and understanding of how to stay safe and risk free. Change wording to 'Limit the Risk'
- To ensure risks are identified, assessed, and mitigated (where possible) in order to reduce any possibility of harm to the student or liability to the schools or Trust.

This policy is available for anybody to read on each academy website. For clarity, the e-safety policy uses the following terms unless otherwise stated:

Users - refers to staff, board of directors, local governing body, Academy volunteers, students and any other person working in or on behalf of the Academy, including contractors.
Parents – any adult with a legal responsibility for a child/young person who is a student at an Academy within the Trust e.g. parent, carer, guardian.
Academy – any Academy business or activity conducted on or off the Academy site, e.g. visits, conferences, Academy trips etc.
Wider Academy community – students, all staff, board of directors, local governing body, parents**.**

ROLE OF THE BOARD OF DIRECTORS

The board of directors are accountable for ensuring that each school has effective policies and procedures in place. As such they will:

- Review this policy at least annually and in response to any changes in requirements or legislation to ensure that the policy is up to date, covers all aspects of technology use within academies, to ensure e-safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.

ROLE OF HEADTEACHERS

Reporting to the board of directors, the Headteacher has overall responsibility for e-safety within each Academy. The day-to-day management of this will be delegated to the e-Safety Officer/Designated Safeguarding Lead of each academy and will be updated annually on their website.

The Headteacher will ensure that:

- E-Safety training throughout the schools is planned, up to date and appropriate to the recipient, i.e. students, all staff, senior leadership team, board of directors, local governing body and parents
- The designated safeguarding lead has had appropriate CPD in order to undertake the day to day responsibilities
- All e-safety incidents are dealt with promptly and appropriately

The Responsible Designated Safeguarding Lead will:

- Keep up to date with the latest risks to children whilst using technology; familiarise themselves with the latest research and available resources for each Academy and home use
- Review this policy regularly and bring any matters to the attention of the Headteacher
- Advise the Headteacher and board of directors on all e-safety matters
- Engage with parents and the Academy community on e-safety matters at the Academy and/or at home
- Liaise with the local authority, IT technical support and other agencies as required
- Retain responsibility for the e-safety incident log; ensure staff know what to report and ensure the appropriate audit trail

- Ensure any technical e-safety measures in the Academy (e.g. internet filtering software, behaviour management software) are fit for purpose, through liaison with the local authority and/or IT technical support
- Make themselves aware of any reporting function with technical e-safety measures, i.e. internet filtering reporting function, liaise with the Headteacher and responsible local governor to decide on what reports may be appropriate for viewing

ROLE OF IT TECHNICAL SUPPORT STAFF

Technical support staff are responsible for ensuring that:

The IT technical infrastructure is secure. This will include as a minimum:

- Anti-virus is fit-for-purpose, up to date and applied to all capable devices
- Windows (or other operating system) updates are regularly monitored, and devices updated as appropriate
- Any e-safety technical solutions, such as internet filtering, are operating correctly
- Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the Headteacher
- Passwords are applied correctly to all users regardless of age

ROLE OF ALL STAFF WORKING WITH STUDENTS

Staff ensure that:

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the e-Safety Officer/Designated Safeguarding Lead
- Using suitable software for teaching staff to monitor student activity in the classroom environment. Attend Training sessions in how to use the software to support engagement in the lesson.
- Any e-safety incident is reported to the DSL if appropriate, or in his/her absence the Headteacher, and report completed on Safeguard. If they are uncertain about an incident, the matter is referred to the DSL, who will make a decision on whether it is classed as an e-safety incident
- The reporting flowcharts contained within this e-safety policy are fully understood

ROLE OF PARENTS AND CARERS
Parents play the most important role in the development of their children; as such each Academy will ensure that parents have the skills and knowledge, they need to ensure the safety of children outside their Academy environment. Through parents' evenings, the Academy newsletters, and the designated page on the website *each* Academy will keep parents up to date with new and emerging e-safety risks and will involve parents in strategies to ensure that students are empowered.

Parents will have the opportunity to attend E Safety Sessions with members of the safeguarding team. Parents will be supported with understanding the age restrictions for electronic systems and apps and how to remove and monitor access to their child's device.

Parents must also understand and support the Academies in upholding the rules it has in place to ensure that their child can be properly safeguarded.

Parents can be blocked on Social Media for their conduct towards the school's official channel. This trust will send a letter to the parent to explain the decision.

Parents will be invited into school for a meeting to discuss unacceptable use of Social media and could be reported to the Police or a MASH referral to be submitted. Issues that could be deemed as unacceptable are:

- Sending abuse to a member of staff or harassing online
- Sharing false information about the school or a member of staff
- Contacting a student electronically and harassing or being abusive
- This list is not exhaustive, and any other behaviour deemed unacceptable by the Headteacher, Deputy Headteacher, DSL, DDSL or Governing Body.

INFORMATION FOR ALL STUDENTS
The guidelines on agreed use of IT equipment and services in the academies are given in the 'Student Acceptable Use Policy'; any deviation from this policy or misuse of IT equipment or services will be dealt with in accordance with the behaviour policy.

E-Safety is embedded into our curriculum; students will be given the appropriate advice and guidance by staff. Similarly, all students will be fully aware of how they can report areas of concern whilst at their Academy or outside of Academy.

Online Bullying and Harassment in the Schools Bullying policy has a further detail

TECHNOLOGY
The Wellington schools use a range of devices including PCs, laptops, and tablets. In order to safeguard the student and in order to prevent the loss of personal data we employ the following assistive technology:

Internet Filtering – we use a firewall and internet filtering system that prevents unauthorised access to illegal or inappropriate websites. Appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to a change in requirements or legislation, whichever is sooner. The IT Coordinator, e-Safety Officers and IT Support are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Headteacher.

Email Filtering – we use filters that prevent any infected email being sent from or received. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message.

Encryption – all school owned devices that hold personal data (as defined by the Data Protection Act 2018) are encrypted. No data leaves the internal systems on an un-encrypted device; all devices that are kept on the site and which may contain personal data are encrypted. Any breach (i.e. loss/theft of device such as laptop or USB key drives) is to be brought to the attention of the Head teacher immediately. The Headteacher will liaise with the Data Protection Officer to ascertain whether a report needs to be made to the Information Commissioner's Office.

Passwords – all staff and students will be unable to access any device without a unique username and password. Staff passwords will change every 45 days and student every 150 days or if there has been a compromise, whichever is sooner. The IT Support team will be responsible for ensuring that passwords are changed.

Anti-Virus – all capable devices will have anti-malware software. This software is updated as and when virus definitions are available. Tech IT will be responsible for ensuring this task is carried out and will report to the Headteacher if there are any concerns. The Academies discourage the use of USB devices and are blacklisted on the network.

SAFE USE OF EQUIPMENT AND THE INTERNET

Internet – Use of the Internet is a privilege, not a right. Internet use will be granted to staff upon acceptance of the policy, staff are required to indicate they accept the terms of the policy each time they log-on to a computer. Parents will be contacted with the details of the infringement and the amount of time that their internet access is restricted. Teaching staff will be contacted and Student Managers when a student's internet or student access is restricted. This will allow staff to plan for the student when using an IT Room. The infringement will be logged on SIMS in the child's behaviour record.

Email – All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Similarly use of personal email addresses for work purposes is not permitted. Students are permitted to use email, and as such will be given their own email address. Students will be trained how to use their email address and understand email etiquette. This will be revisited when there is any issues or poor behaviour with the student.

Mobile phone – Staff are encouraged not to use their own personal device to call parents. If they need to use their device, then they should block their number. (In an event it is necessary to keep in contact with the parent sharing your number will be authorised by the Headteacher or Deputy Headteacher). Texting or other personal apps will not be used for communication via a personal device.

TEAMS will be used as our school's VLE and has been set up to respond to the COVID-19 school closure. The following have been set up to ensure all using the system are safeguarded

- Teams will be used to share and upload files
- Files shared we will hold the copyright for or have purchased the rights to share electronically
- Students cannot communicate with each other through the system or staff
- Students cannot call via the system
- Live lessons are set and secured so students can not take control
- Student accounts have set that they are subordinate to staff accounts and restricted to access and uploaded their own work.

Photos and videos come under sensitive personal data within GDPR. All parents have access to an "opt-in" form for photo usage. If the signed forms are not received back the student is considered as not giving consent and will not be included in photos.

Social Networking – there are many social networking services available; the academies are fully supportive of social networking as a tool to engage and collaborate with learners, and to engage with parents and the wider Academy community. The following social media services are permitted for use within the Trust:

(the terms and conditions of the service will always be adhered to. For example, no student under 14 will be asked to access Facebook or Twitter)

- Twitter – used by academies as a broadcast service (see below)
- Facebook – also used by academies as a broadcast service (see below)

A broadcast service is a one-way communication method in order to share Academy information with the wider Academy community. No persons will be "followed" or "friended" on these services and as such no two-way communication will take place. In addition, the following is to be strictly adhered to:

- The photographic consent section of the schools MIS must be consulted before any image or video of any child is uploaded
- There is to be no identification of students using first name and surname; first name only is to be used
- Where services are "comment enabled", comments where possible are to be set to "moderated"
- All posted data must conform to copyright law; images, videos and other resources that are not originated by the Trust schools are not allowed unless the owner's permission has been granted or there is a licence which allows for such use

Notice and take down policy – should it come to the school's attention that there is a resource which has been inadvertently uploaded, and copyright permission has not been secured to use that resource, it will be removed within one working day.

TRAINING AND CURRICULUM

It is important that the wider community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. As such, the schools will have an annual programme of training which is suitable to the audience.

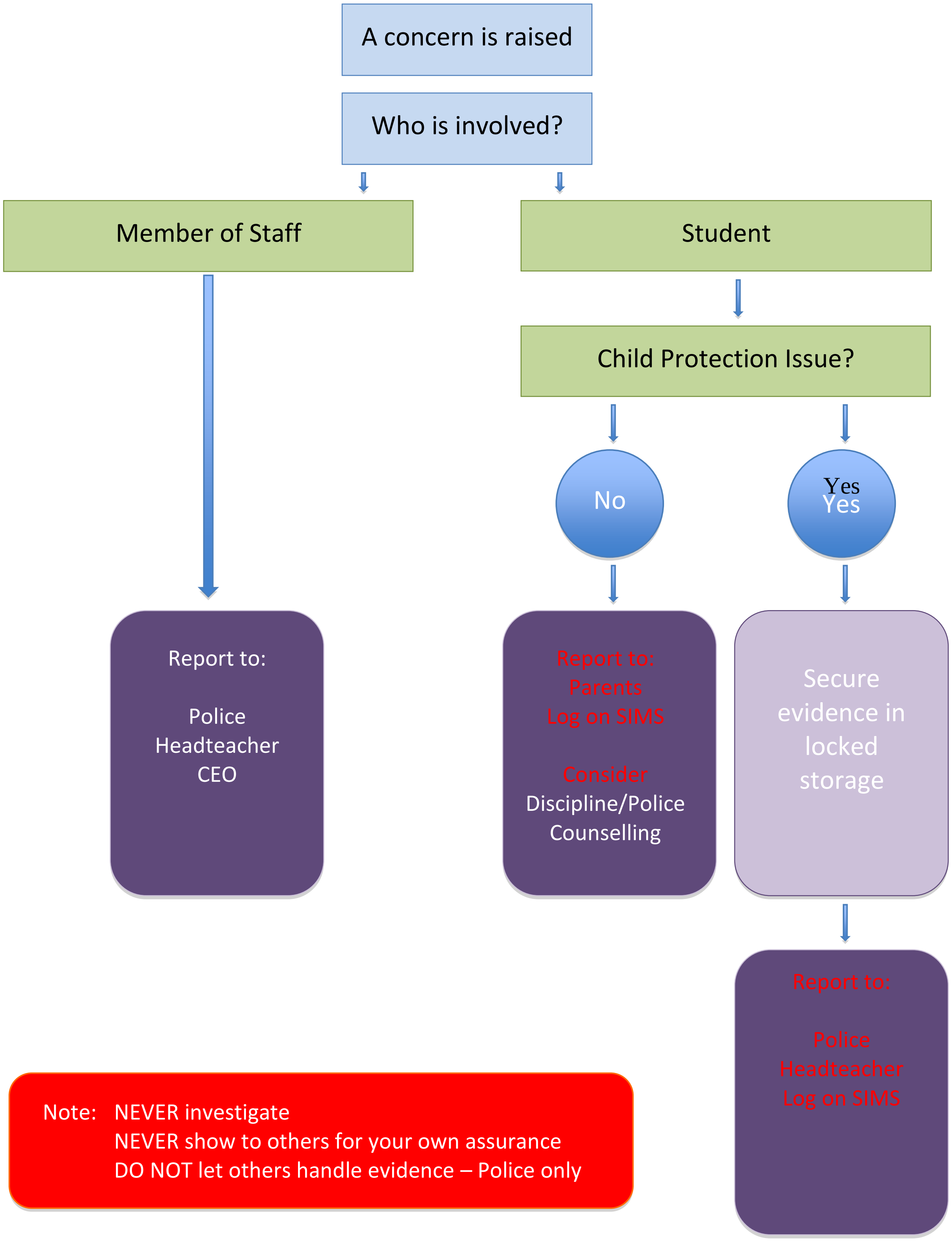
E-Safety for students is embedded into the curriculum; whenever IT is used, staff will ensure that there are positive messages about the safe use of technology and risks as part of the student's learning.

Students in Key Stage 3 (year 7 and 8) each spend one term exploring e-safety issues. Further details are available in the KS3 SOW for Computing and IT and Sub Curriculum provision.

E-safety is also embedded in the KS3 and KS4 Well-being curriculum and is taught alongside issues such as bullying and self-harm. Regular assemblies are delivered to each year group to remind all students of the need to stay safe online.

Recording student issues on SIMS section could be added here or in the Bullying Policy

Illegal Activity Flowchart



A concern is raised

Who is involved?

Member of Staff

Student

Child Protection Issue?

No

Yes
Yes

Report to:

Police
Headteacher
CEO

Report to:
Parents
Log on SIMS

Consider
Discipline/Police
Counselling

Secure evidence in locked storage

Report to:

Police
Headteacher
Log on SIMS

Note: NEVER investigate
NEVER show to others for your own assurance
DO NOT let others handle evidence – Police only