WELLINGTON COLLEGE
SPONSOR OF
WELLINGTON COLLEGE ACADEMY TRUST

E-SAFETY POLICY

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

DOCUMENT CONTROL	
Responsible position:	**Approved by:**
I.T. Director	Executive Principal
Version number:	**Date approved:**
V1.1	March 2017
Review Period:	**Next review date:**
Annually	March 2018

RELATED POLICIES AND DOCUMENTS	
Policy Name	**Date Issued**
Safeguarding and Child Protection Policy	June 2014
Freedom of Information Policy	June 2014
Equal Opportunities Policy	June 2013
Behaviour of Learning and Principles Policy	June 2013
Health and Safety Policy	June 2013
National Minimum Standards - Appendix 1/1; revision Sept 2014 Revised NMS	January 2013 May 2015

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

INTRODUCTION

Safeguarding is a serious matter; within the Wellington College Academy Trust 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 Trust community is provided with the knowledge and understanding of how to stay safe and risk free.
- 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 Trust.

This policy is available for anybody to read on the Wellington College Academy Trust and 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, Trust / Academy volunteers, students and any other person working in or on behalf of the Trust /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 / Trust business or activity conducted on or off the Academy /Trust 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 our Trust 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 the Trust, to ensure e-safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.

ROLE OF THE EXECUTIVE PRINCIPAL

Reporting to the board of directors, the Executive Principal has overall responsibility for e-safety within the Trust. The day-to-day management of this will be delegated to the e-Safety Officer/Child Protection officerof each academy and will be updated annually on their website.

The Executive Principal will ensure that:

- E-Safety training throughout the Trust 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 e-Safety Officer(s) has had appropriate CPD in order to undertake the day to day responsibilities

- All e-safety incidents are dealt with promptly and appropriately

E-SAFETY OFFICERS

The responsible e-Safety Officer 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 Executive Principal / Head teacher
- Advise the Executive Principal 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 Executive Principal 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 e-Safety Officers and Executive Principal
    - 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 Officers
- Any e-safety incident is reported to the e-Safety Officers, or in his/her absence the Executive Principal/ Head of Academy, and an e-Safety Incident report is completed. If they are uncertain about an incident, the matter is referred to the e-Safety Officers, 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 must also understand and support the Trust in upholding the rules it has in place to ensure that their child can be properly safeguarded.

INFORMATION FOR ALL STUDENTS

The guidelines on agreed use of IT equipment and services in the Trust 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 Trust's 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.

THE E-SAFETY COMMITTEE

Each academy will have an e-safety committee which will be established from volunteer students, parents, the e-Safety Officers, responsible Local Governor and others as required the e-Safety Committee will meet at least three times a year. The e-Safety Committee is responsible for:

- Advising on changes to the e-safety policy
- Establishing the effectiveness of e-safety training and awareness in the Academy
- Recommending further initiatives for e-safety training and awareness at the Academy

TECHNOLOGY

Wellington College Academy Trust uses a range of devices including PCs, laptops, tablets and Apple Macs. 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 software that prevents unauthorized 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 Executive Principal/ Head of Academy.

Email Filtering – we use software that prevents any infected email being sent from or received by the Trust. 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 Trust devices that hold personal data (as defined by the Data Protection Act 1998) are encrypted. No data leaves the Trust on an un-encrypted device; all devices that are kept on Trust property 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 Executive Principal/ Head teacher immediately. The

Executive Principal/ Head teacher will liaise with the Data Officer of the Trust 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 and student passwords will change on a termly basis 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-virus software. This software will be updated at least weekly for new virus definitions. IT Support will be responsible for ensuring this task is carried out, and will report to the Executive Principal if there are any concerns. All USB peripherals such as key drives are to be scanned for viruses before use.

SAFE USE OF EQUIPMENT AND THE INTERNET

Internet – Use of the Internet within the Trust 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.

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 the Trust email system, and as such will be given their own email address.

Photos and videos –All parents have access to an "opt out" form which is available for download in the parents section of the website.

Social Networking – there are many social networking services available; the Trust is 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:

- Blogging – used by staff and students in the Trust
- Twitter – used by the Trust as a broadcast service (see below)
- Facebook – used by the Trust 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 "No Photo" section of the Trust's 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 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 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 Trust's attention that there is a resource which has been inadvertently uploaded, and the Trust does not have copyright permission to use that resource, it will be removed within one working day.

TRAINING AND CURRICULUM

It is important that the wider Trust 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 Trust 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 in the Trust, 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. In year 7 they will publish various documents offering advice and guidance on the risks, in year 8 students will use movie maker or similar software to create a short advice film.

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.

Appendix 1 – Student friendly poster displayed in all ICT rooms

Appendix 2 – E-safety incident form

Appendix 3 – Flow charts for reporting an incident

APPENDIX 1 – DISPLAYED IN ALL ICT ROOMS

Our Charter of Good Online Behaviour

Note: All Internet and email activity is subject to monitoring

I Promise – to only use the Academy ICT for school work that the teacher has asked me to do.

I Promise – not to look for or show other people things that may be upsetting.

I Promise – to show respect for the work that other people have done.

I will not – use other people's work or pictures without permission to do so.

I will not – damage the ICT equipment, if I accidentally damage something I will tell my teacher.

I will not – share my password with anybody. If I forget my password I will let my teacher know.

I will not – use other people's usernames or passwords.

I will not – share personal information online with anyone.

I will not – download anything from the Internet unless my teacher has asked me to.

I will – let my teacher know if anybody asks me for personal information.

I will – let my teacher know if anybody says or does anything to me that is hurtful or upsets me.

I will – be respectful to everybody online ; I will treat everybody the way that I want to be treated.

I understand – that some people on the Internet are not who they say they are, and some people can be nasty. I will tell my teacher if I am ever concerned at school, or my parents if I am at home.

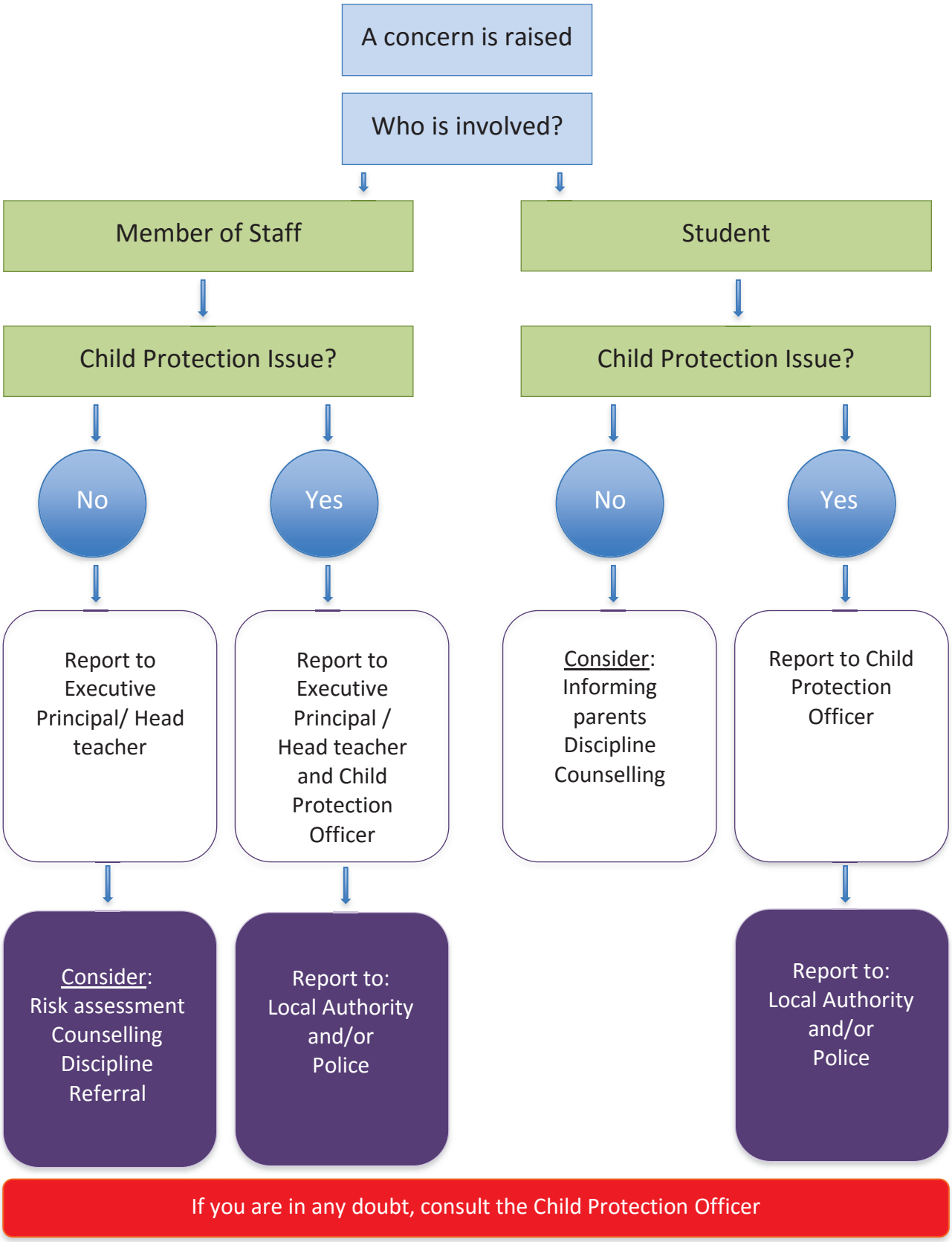
I understand – if I break the rules in this charter there will be consequences of my actions

APPENDIX 2 – E-SAFETY INCIDENT LOG

Number:	**Reported By:**	**Reported To:**
	When:	**When:**
Incident Description: (Describe what happened, involving which children and/or staff, and what action was taken)		
Review Date:		
Result of Review:		
Signature e-safety officer		**Date:**
Signature Child Protection officer		**Date:**

APPENDIX 3

Inappropriate Activity Flowchart



Illegal Activity Flowchart