Welland Park Academy

E-SAFETY POLICY

Reference this policy is aligned to with LCC	**xx.xx.xx**
Agreed with Support Staff Trade Unions	**Xx.xx.xx**
Adopted by the Governing Body	**Sep 2020**
Next Review Due	**Jun 2022**
Agreed with Teacher Trade Unions and Professional Associations	**xx.xx.xx**

Introduction

For clarity, the E-safety policy uses the following terms unless otherwise stated:

Users – refers to staff, governing body, school volunteers, students and any other person working in or on behalf of the school, including contractors

Parents – any adult with a legal responsibility for the child/young person outside the school e.g parents, guardian, carer

School – any school business or activity conducted on or off school site, e.g visits, conferences, school trips etc

Wider school community – students, all staff, governing body, parents, volunteers

Safeguarding is a serious matter: at Welland Park Academy 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 a bi-ennial basis or in response to an e-safety incident, whichever is sooner.

The primary purpose of the policy is twofold:

- To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to the student or liability to the school

- This policy is available for anybody to read on the Welland Park Academy website; annually all members of staff will electronically sign as read and understood. A copy of this policy and the Student Use of ICT Agreement will be sent home via forms for electronic signature. Upon return of the signature and acceptance of the terms and conditions, students will be permitted access to school technology including the internet.

Policy Governance (Roles and Responsibilities)

Governing Body

The governing body is accountable for ensuring that our school has effective policies and procedures in place; as such they will:

- Review this policy at least bi-ennially and in response to any e-safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure e-safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents
- Appoint one governor to have overall responsibility for the governance of e-safety at the school who will:
  - Keep up to date with emerging risks and threats through technology use
  - Receive regular updates from the Principal in regards to training, identified risks and any incidents
  - Chair the Student Wellbeing Committee

Principal

Reporting to the governing body, the Principal has overall responsibility for e-safety within our school. The day to day management of this will be delegated to a member of staff, the E-Safety Officer, as indicated below.

The Principal will ensure that:

- E-safety training throughout the school is planned and up to date and appropriate to the recipient, i.e students, all staff, senior leadership team and governing body, parents
- The designated E-Safety Officer (s) has had appropriate CPD in order to undertake the day to day duties
- All e- safety incidents are dealt with promptly and appropriately

E-Safety Officer

The day to day duty of the E-Safety Officer is devolved to the designated safeguarding lead.

The E-Safety Officer will:

- Keep up to date with the latest risks to children whilst using technology; familiarise him/herself with the latest research and available resources for school and home use
- Review this policy regularly and bring any matters to the attention of the Principal
- Advise the Principal and governing body of all e-safety matters
- Engage with parents and the school community on e-safety matters at school 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 school (e.g internet filtering software, behaviour management software) are fit for purpose through liaison with the local authority and/or ICT Technical Support
- Make him/herself aware of any reporting function with technical e-safety measures, i.e internet filtering reporting function; liaise with the Principal and responsible governor to decide on what reports may be appropriate for viewing

ICT Technical Support Staff

Technical support staff are responsible for ensuring that:

- The IT technical infrastructure is secure; this will include at 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 or use are discussed and agreed with the E-Safety Officer and Principal
  - Passwords are applied correctly to all users regardless of age. Passwords for staff will be a minimum of 8 characters

All Staff

Staff are to ensure that:

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the Principal

- Any e-safety incident is reported to the E-Safety Officer (and an e-safety incident report is made), or in his/her absence to the Principal. If you are unsure the matter is to be raised with the E-Safety Officer of the Principal to make a decision
- The reporting flowcharts contained within this e-safety policy are fully understood

All Students

The boundaries of use of ICT equipment and services in this school are given in the Student Use of ICT Agreement; any deviation or misuse of ICT 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 how they can report areas of concern whilst at school or outside of school.

Parents and Carers

Parents play the most important role in the development of their children; as such the school will ensure that parents have the skills and knowledge they need to ensure the safety of children outside the school environment. Through parents' evening, school newsletters, Schoolcomms, the school 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 the school needs to have rules in place to ensure that their child can be properly safeguarded. As such parents will electronically sign the Student Acceptable Use Policy before any access can be granted to school ICT equipment or services.

Student Wellbeing Committee

Chaired by the senior leader responsible for Well Being, the Student Council is responsible:

- To advise on changes to the e-safety policy
- To establish the effectiveness (or not) of e-safety training and awareness in the school
- To recommend further initiatives for e-safety training and awareness at the school

Established from volunteer students, parents, E-Safety Officer, responsible Governor and others as required, the Student Council will meet regularly.

Technology

Welland Park Academy uses a range of devices including PCs, laptops, Apple Macs, and ipads. In order to safeguard the student and in order to prevent loss of personal date we employ the following assistive technology:

Internet Filtering – we use relevant software that prevents unauthorised access to illegal websites. It also prevents access to 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 an incident, whichever is sooner. The ICT Manager, E-Safety Officer and IT Support are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Principal.

Email Filtering – we use appropriate software that prevents any infected email to be sent from the school, or to be received by the school. 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.

Passwords – all staff and students will be unable to access any device without a unique username and password.

Anti-Virus – all capable devices will have anti-virus software installed. 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 Principal if there are any concerns. All USB peripherals such as keydrives are to be scanned and labelled as checked for viruses before use. No unchecked USB devices are allowed to be used on site.

Safe Use

Internet – use of the internet in school is a privilege, not a right. Internet use will be granted; to staff upon signing this e-safety policy and the Staff Acceptable Use Policy; students upon signing and returning their acceptance of the Acceptable Use Policy.

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 or personal email addresses for work purposes is not permitted.
Students are permitted to use the school email system, and as such will be given their own email address.

Photos and Videos – digital media such as photos and videos are covered in the schools' Photographic Policy, and is reiterated here for clarity. All parents must sign a photo/video slip on admission.

Social Networking – there are many social networking services available; Welland Park Academy is fully supportive of social networking as a tool to engage and collaborate with learners, and to engage with parents and the wider school community. The following social media services are permitted for use within Welland Park Academy and have been appropriately risk assessed; should staff wish to use other social media, permission must first be sought via the E-Safety Officer who will advise the Principal for a decision to be made. Any new service will be risk assessed before use is permitted.

- Blogging – used by staff and students in school
- Twitter – used by the school as a broadcast service (see below)
- Whatsapp – used by discrete groups for communication
- Facebook – used to promote school and some communications

A broadcast service is a one-way communication method in order to share school information with the wider school 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:

- Permission slips (via the school photographic policy) 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 school are not allowed unless the owner's permission has been granted or there is a licence which allows for such use (i.e creative commons)

Notice and take down policy

Should it come to the schools' attention that there is a resource which has been inadvertently uploaded and the school does not have copyright permission to use that resource, it will be removed within one working day.

Incidents – any e-safety incident is to be brought to the immediate attention of the E-Safety Officer, or in his/her absence the Principal. The E-Safety Officer will assist you in taking the appropriate action to deal with the incident and to fill out an incident log.

Training and Curriculum – it is important that the wider school 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, Welland Park Academy will have an annual programme of training which is suitable to the audience.

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

As well as the programme of training we will establish further training or lessons as necessary in response to any incidents.

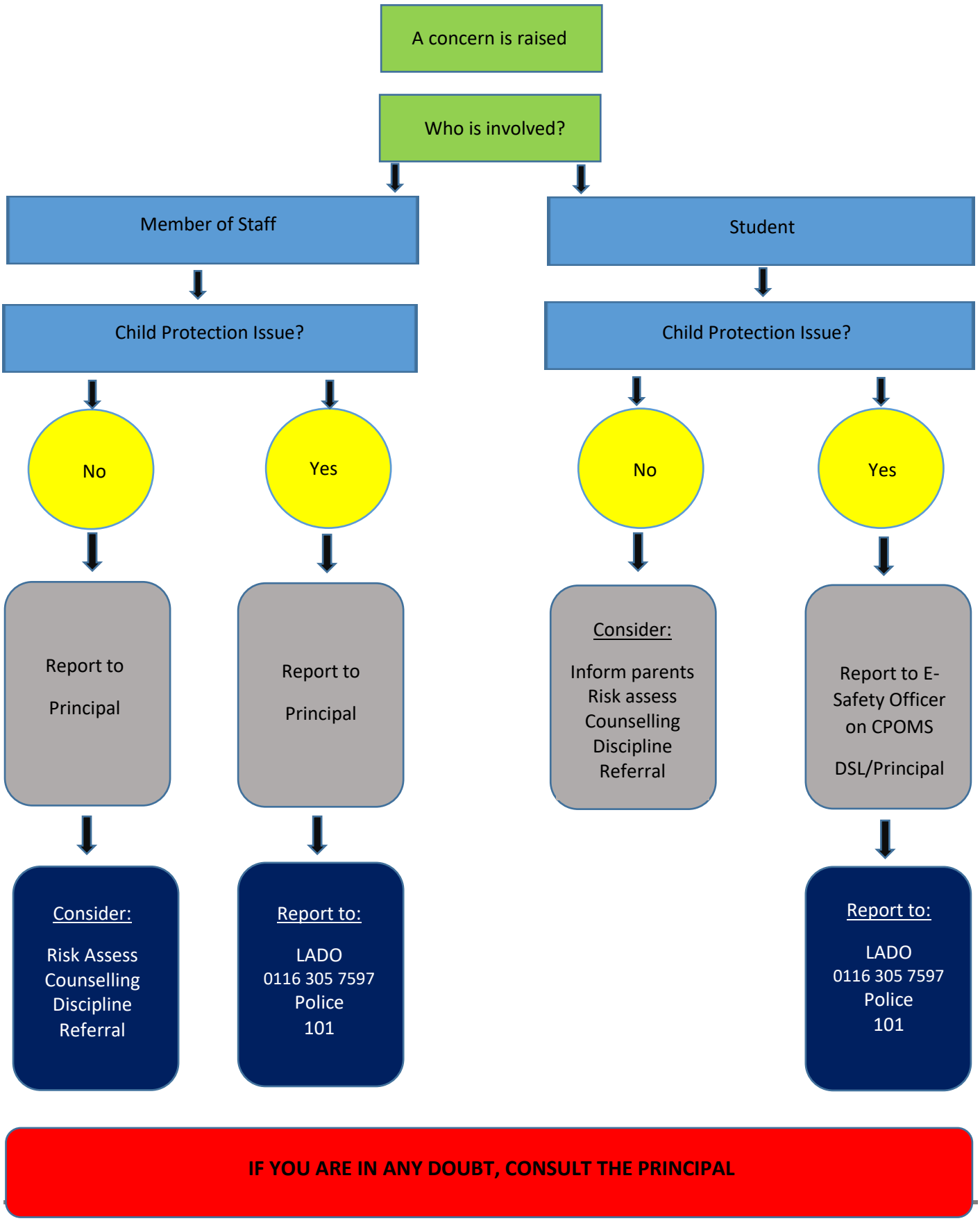
The E-Safety Officer is responsible for recommending a programme of training and awareness for the school year to the Principal and responsible Governor for consideration and planning. Should any member of staff feel they have had inadequate or insufficient training generally or in any particular area, this must be brought to the attention of the Principal for further CPD.

E-Safety Incident Log

Number:	**Reported By:** (name of staff member)	**Reported To:** (e.g Principal, E-Safety Officer)
	When:	**When:**
Incident Description: (Describe what happened, involving which children and/or staff, and what action was taken)		
Review Date:		
Result of Review:		

Signature: (Principal)		**Date:**	
Signature: (Governor)		**Date:**	

Inappropriate Activity Flowchart



ILLEGAL ACTIVITY FLOWCHART