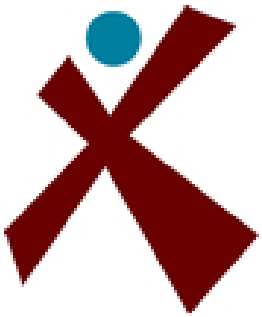
Sprowston Community Academy
E-Safety Policy



September 2018

Contents

Policy Statement

The purpose of the policy is to identify and mitigate risk to reduce any foreseeability of harm to the student or liability to the school. This will be achieved by defining the boundaries of appropriate and inappropriate use of technology through effective education and training to both staff and students to ensure the whole school community has the knowledge to stay safe online and know reporting mechanisms.

Safeguarding is a serious matter; at SCHS 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 an e-safety incident, whichever is sooner.

This policy is available for anybody to read on the SCHS website and is located in the Policies folder. A copy of the Students Acceptable Use Policy will be sent home with to prospective Year 6 students for them to sign for their Year 7 start. Upon return of the signed permission slip and acceptance of the terms and conditions, students will be permitted access to school technology including the Internet. In addition all Staff members will be required to sign a copy of the Staff Acceptable Use Policy.

Headteacher Name: Andrew John **Signed:**

Review Date:

Policy Governance (Roles & Responsibilities)

- The e-Safety Officer will review this policy regularly or 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.

Headteacher

Reporting to the governing body, the Headteacher 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 (or more than one), as indicated below.

The Headteacher 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 e-Safety Officer will:

- Keep up to date with the latest risks to children whilst using technology; familiarize 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 Headteacher.
- Advise the Headteacher, governing body on 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 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 Headteacher and responsible governor to decide on what reports may be appropriate for viewing.
- Ensure e-Safety for 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. e-Safety should be focused on developing awareness and not restriction and prevention rather than cure.
- be responsible for recommending a programme of training and awareness for staff which should be responsive to staff knowledge and developments in technology.

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.
    - 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.

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 Headteacher.
- Any e-safety incident is reported to the e-Safety, or in his/her absence to the Headteacher or Deputy Headteacher for safeguarding.. If you are unsure the matter is to be raised with the e-Safety Officer or the Headteacher/Deputy Headteacher 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 Acceptable Use Policy; 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. The curriculum and advice given will be updated regularly to reflect the current trends of Internet and Mobile Phone use. 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' evenings, and the school website 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 have to rules in place to ensure that their child can be properly safeguarded. As such parents will sign the student Acceptable Use Policy before any access can be granted to school ICT equipment or services.

Technology

Sprowston Community High School uses a range of devices including PC's, laptops and tablets. In order to safeguard the student and in order to prevent loss of personal data we employ the following assistive technology:

Internet Filtering – we use DofE approved software that prevents unauthorized 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. IT Support are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Headteacher. However, IT Support will allow websites through staff request if it is deemed appropriate through evaluation of web content.

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

Anti-Virus – All capable devices will have anti-virus software IT Support will be responsible for updating the anti-virus software, and will report to the Headteacher if there are any concerns. All USB peripherals such as key drives (if you allow them) are to be scanned for viruses before use.

Safe Use

Internet – Use of the Internet in school is a privilege, not a right. Internet use will be granted: to staff upon reading this e-safety policy and signing 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. 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 must be removed from individual devices and stored in a safe, central location.

Social Networking – there are many social networking services available; Sprowston Community High School 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 Sprowston Community High School and have been appropriately risk assessed; should staff wish to use other social media, must seek advice from IT Support or E-Safety Officer for a decision to be made. Any new service will be risk assessed before use is permitted.

- Blogging e.g. Blogger – used by staff and students in school.
- Twitter – used by the school as a broadcast service (see below).

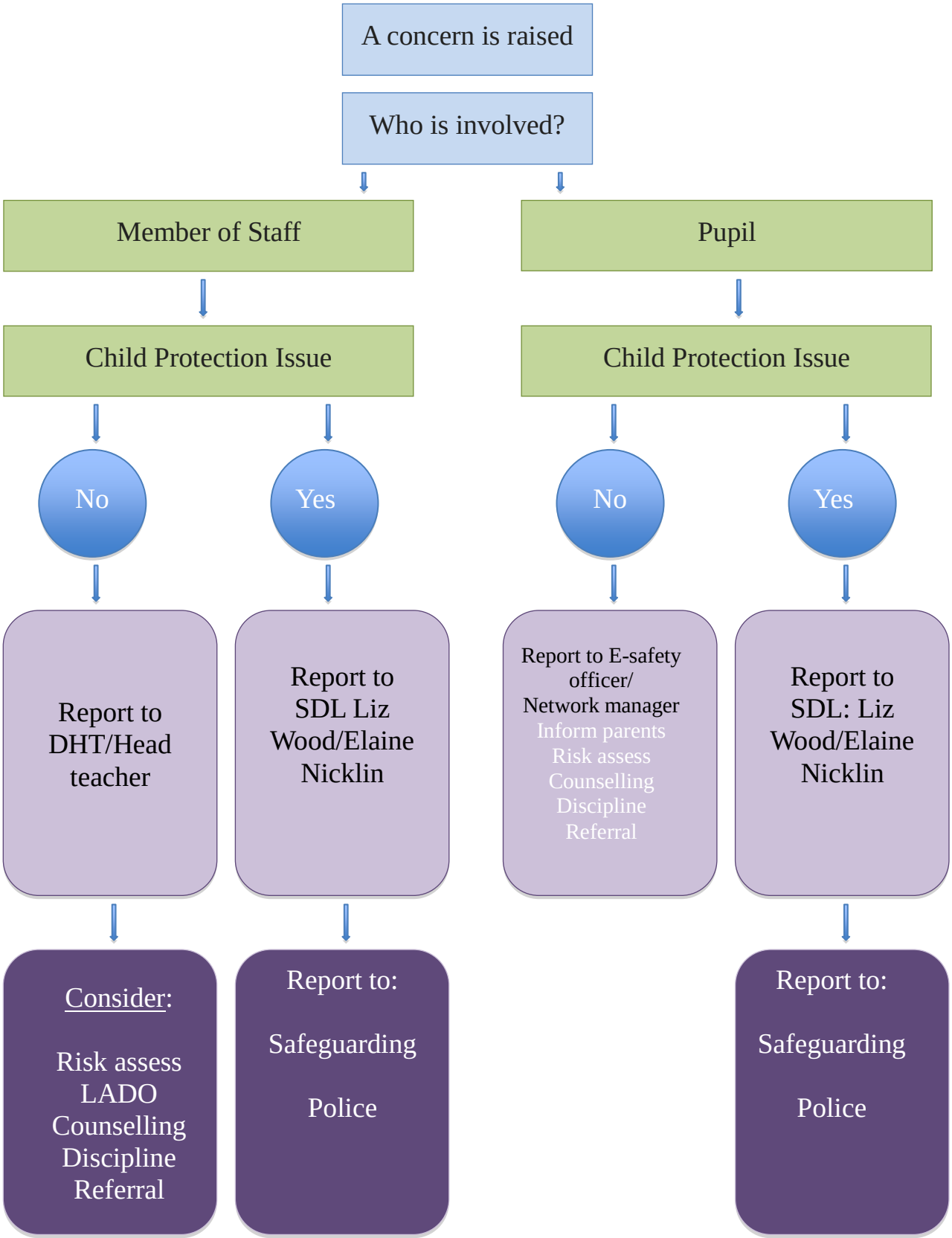
In addition, the following is to be strictly adhered to:

- Permission slips (via the school photographic policy) must be consulted before any image or video of any child is uploaded.
- 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.

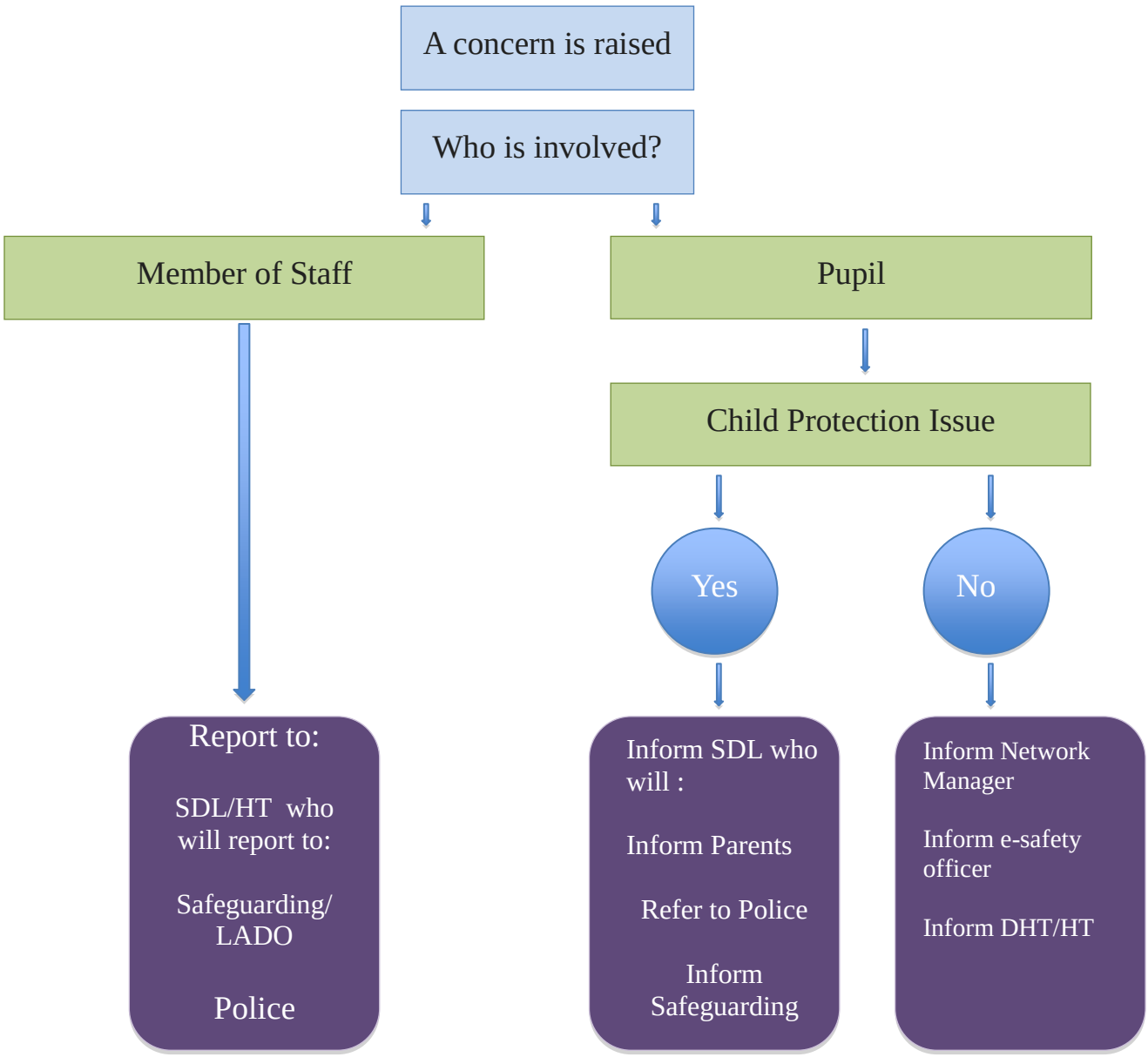
Incidents - Any e-safety incident is to be brought to the attention of the e-Safety Officer, the ICT Network Manager and the Deputy Headteacher. Where appropriate, information will be shared with the Headteacher. The e-Safety Officer will assist you in taking the appropriate action to deal with the incident.

Inappropriate Activity Flowchart



If you are in any doubt, consult the Headteacher and Senior Safeguarding Designated Lead, Liz Wood

Illegal Activity Flowchart



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