William Law C E Primary School

Online Safety

Policy shared with staff on 1st February 2017 by intranet

Policy confirmed by the Governing Body of William Law CE Primary School on:

Date: 31st January 2018

Signature: Anna Bertou

Policy to be reviewed on: January 2021

This policy is written in line with the Christian values and ethos of our school

Policy Statement

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

Users - refers to staff, governing body, school volunteers, pupils 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. parent, guardian, carer.

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

Wider school community – in general to include pupils, all staff, governing body, parents, volunteers.

Safeguarding is a serious matter; at William Law CE Primary School we use technology and the Internet extensively across all areas of the curriculum. Online safeguarding, known as online 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 online safety incident, whichever is sooner.

The primary purpose of this 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 pupil or liability to the school.

This policy is available for anybody to read on the school website; upon review all members of staff will sign as read and understood both the online safety policy and the Staff Acceptable Use Policy.

The Pupil's Acceptable Use Policy will be sent home with pupils at the beginning of each school year with a permission slip. Upon return of the signed permission slip and acceptance of the terms and conditions, pupils will be permitted access to school technology including the Internet.

Policy Governance (Roles & 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 annually and in response to any online safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure online 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 online safety at the school who will:
    - Keep up to date with emerging risks and threats through technology use.
    - Receive regular updates from the Headteacher in regards to training, identified risks and any incidents.
    - Chair the Online Safety Committee

Headteacher

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

The Headteacher will ensure that:

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

Online Safety Officer

The day-to-day duty of online safety Officer is devolved to a Learning Mentor.

The Online 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 online safety matters.
- Engage with parents and the school community on online 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 online safety incident log; ensure staff know what to report and ensure the appropriate audit trail.

- Ensure any technical online safety measures in school (e.g. Internet filtering software, behaviour management software) are fit for purpose through liaison with the local authority and/or IT Technician.
- Make him/herself aware of any reporting function with technical online 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.

IT Technician

The IT Technician is responsible for ensuring that:

- The IT technical infrastructure is secure; this will include at a minimum:
  o Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
  o Windows (or other operating system) updates are regularly monitored and devices updated as appropriate.
  o Any online safety technical solutions such as Internet filtering are operating correctly.
  o Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the online safety officer and Headteacher.
  o Passwords are applied correctly to all users regardless of age.
  o Passwords for staff will be a minimum of 8 characters.
  o The IT System Administrator password is to be changed on a regular basis.

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

All Pupils

The boundaries of use of ICT equipment and services in this school are given in the Pupil Acceptable Use Policy; any deviation or misuse of ICT equipment or services will be dealt with in accordance with the behaviour policy.
Online safety is embedded into our curriculum; pupils will be given the appropriate advice and guidance by staff. Similarly all pupils 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, school newsletters, website and twitter the school will keep parents up to date with new and emerging online safety risks.

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 sign the Pupil Acceptable Use Policy at the start of every school year before any access can be granted to school ICT equipment or services.

Online Safety Committee

Chaired by the Governor responsible for online safety, the Online Safety Committee is responsible:

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

Established from Online safety Officer, responsible Governor, ICT Co-ordinators, IT Technician and others as required, the Online Safety Committee will meet on a termly basis.

Technology

William Law CE Primary School uses a range of devices including PC's, laptops, Apple Macs and iPads. In order to safeguard the pupil and in order to prevent loss of personal data we employ the following assistive technology:

Internet Filtering – we use E2BN Protex web filtering system 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. The ICT Coordinator, Online 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 Headteacher.

Email Filtering – we use Sophos Cloud 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.

Encryption – No personal data (as defined by the Data Protection Act 1998) will be stored on un-encrypted devices. All teaching staff are supplied with encrypted USB memory sticks to ensure no data leaves the school on an un-encrypted device; any breach (i.e. loss/theft of device such as laptop or USB memory sticks) is to be brought to the attention of the Headteacher immediately. The Headteacher will liaise with the local authority to ascertain whether a report needs to be made to the Information Commissioner's Office.

Passwords – All staff with access to school networks containing personal data will be unable to connect without using a unique username and password. The school network requires that these passwords are changed on a regular basis otherwise access is denied. Children access limited areas of the network through class user names and passwords. KS2 children using Google Apps for Education are provided with unique user names and passwords.

Anti-Virus – All capable devices will have anti-virus software. This software will be updated at least weekly for new virus definitions. The IT Technician will be responsible for monitoring the status of all devices to ensure they are up-to-date, and will report to the Headteacher if there are any concerns.

Safe Use

Internet – Use of the Internet in school is a privilege, not a right. Internet use will be granted: to staff upon signing the Staff Acceptable Use Policy;
Pupils will be granted access upon signing and/or their parents 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 of personal email addresses for work purposes is not permitted.
KS2 children using Google Apps for Education will be supplied with an email address to use as a user name and for email. The email address will comprise of their graduation year and first name e.g. 2017jack@wlaw.school. Restrictions are in place with pupil's emails to only allow sending and receiving emails within school.

Photos and videos – As part of the school admissions procedure a pupil admission form is completed for any child registered with the school. On this form parents give consent for their child to be photographed or digitally recorded for school purposes. This confirms their understanding that such photographs and videos may be used within the school and on the school website. As part of this agreement the school will ensure that no photographs are accompanied by the child's name. Parents can choose to consent to only to photos and videos being used within school.

Social Networking – there are many social networking services available, William Law has permitted the use of Twitter as a broadcast service within school to engage with parents and the wider school community. 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" on Twitter and as such no two-way communication will take place.

Any new service will be risk assessed before use is permitted.
.

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

- The photo concerns list must be consulted before any image or video of any child is uploaded.
- There is to be no identification of pupils using first name and surname;
- 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).

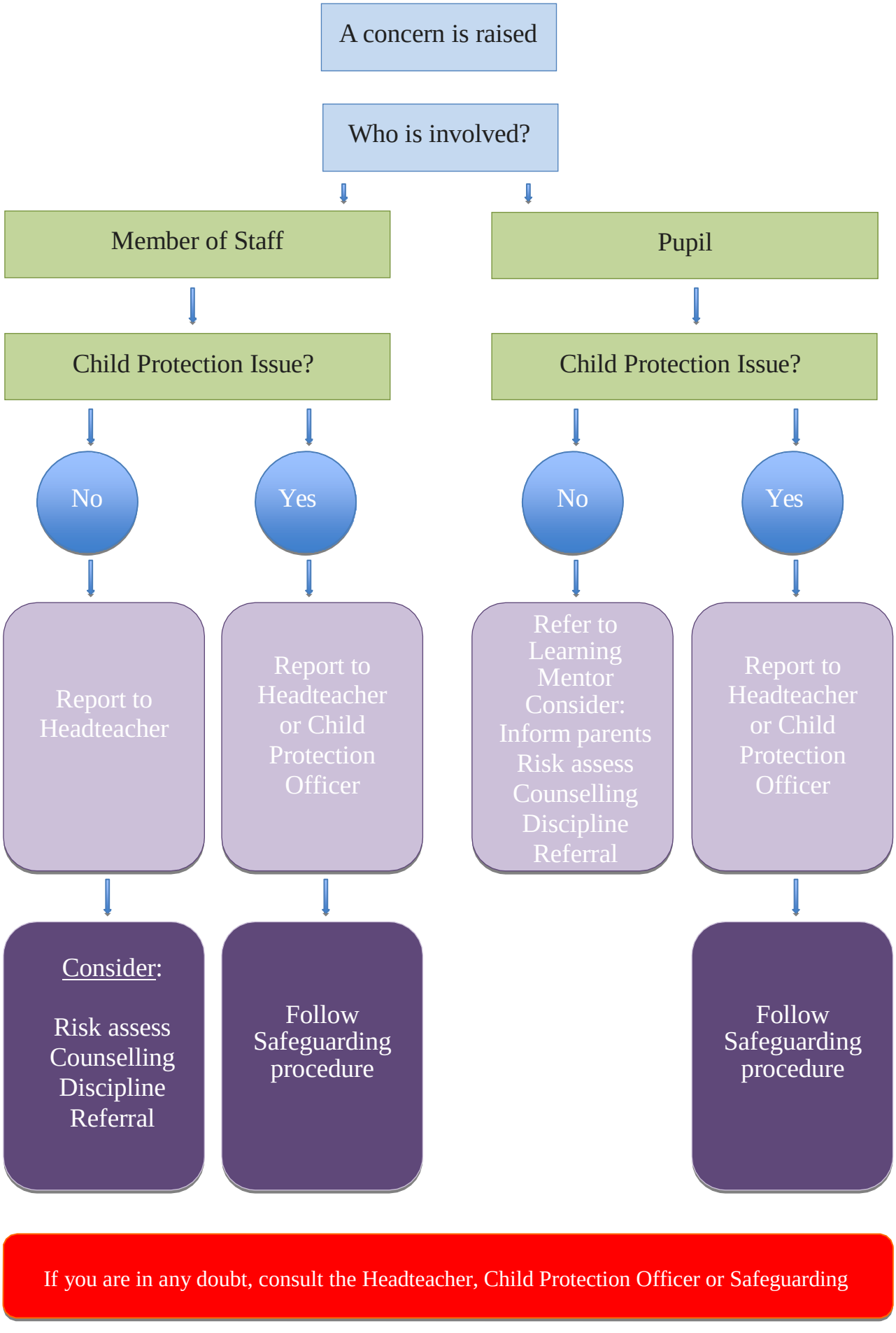
Notice and take down policy – should it come to the school's attention that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed within one working day.

Incidents - Any online safety incident is to be brought to the immediate attention of the Online Safety Officer, or in his/her absence the Headteacher. The Online Safety Officer will assist in taking the appropriate action to deal with the incident and to ensure the incident is logged.

Wider Social Media concerns – Any sexting, child sexual exploitation or sharing of inappropriate images discovered online must be brought to the immediate attention of the Online Safety Officer or in his/her absence the Headteacher. Action is to be taken in accordance to the threshold document or legal action considered if necessary.

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, William Law will have an annual programme of training, which is suitable to the audience. Online safety for pupils 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 pupil's learning.
As well as the programme of training we will establish further training or lessons as necessary in response to any incidents.
The Online Safety Officer is responsible for recommending a programme of training and awareness for the school year to the Headteacher 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 Headteacher for further CPD.

Inappropriate Activity Flowchart



Illegal Activity Flowchart