'Growing together,
Learning forever'

Woodstone Community Primary School

Online Safety Policy

Date: September 2022

Date for review: September 2024

Policy Statement

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. 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 – students, all staff, governing body, parents.

Safeguarding is a serious matter; at Woodstone Community Primary School 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 two-yearly basis or in response to an e-safety incident, whichever is sooner. This policy should be read in conjunction with the Bullying Prevention Policy, Child Protection Policy, Behaviour Policy and the Website Policy.

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 student or liability to the school.

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 every two years 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 (Rachel Barsby-Robinson, Safeguarding 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 Headteacher in regards to training, identified risks and any incidents.

Behaviour, Welfare and Safety Committee of the Governing Body

The Behaviour, Welfare and Safety Committee is responsible for:

- advising on changes to the e-safety policy.
- establishing the effectiveness (or not) of e-safety training and awareness in the school.
- recommending further initiatives for e-safety training and awareness at the school.

Headteacher

Reporting to the governing body, the Headteacher has overall responsibility for e-safety within our school.

The Headteacher, alongside the Computing co-ordinator 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.
- All e-safety incidents are dealt with promptly and appropriately.

Computing co-ordinator

The Computing co-ordinator, supported by the Headteacher 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.
- 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 Headteacher and responsible governor to decide on what reports may be appropriate for viewing.

ICT Technical Support Staff

ICT Technical support at Woodstone is provided by Finch IT Solutions Ltd.

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 of use are discussed and agreed with the Computing co-ordinator and Headteacher.
  - Passwords are applied correctly to all users regardless of age.
  - The IT System Administrator password is to be changed a regular intervals

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 Headteacher (and an e-Safety Incident report is made). If you are unsure the matter is to be raised with the Headteacher to make a decision.
- The reporting flowcharts contained within this e-safety policy are fully understood.

All Students

e-Safety is embedded into our curriculum through our Purple Mash Computing curriculum and Cambridge PSHE 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.

The boundaries of use of ICT equipment and services in this school are taught alongside our Computing curriculum, displayed around the school and conveyed verbally to students whenever ICT equipment is being used. Any deviation or misuse of ICT equipment or services will be dealt with in accordance with the behaviour policy.

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 parent's evenings, school newsletters, information afternoons 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. We will regularly seek parental opinions and input into E-safety development.

Safeguarding

We recognise that technology is a significant component in many safeguarding and wellbeing issues and that children are at risk of abuse online as well as face to face. Staff will always respond if informed that children have been subject to abuse online as well as if they have been involved in sharing indecent images. The DfE guidance "Sharing nudes and semi-nudes: advice for education settings working with children and young people" (Dec 2020) will be used to guide the school's response on a case by case basis.

The key points for staff and volunteers (not including the DSL) being:-

- Report immediately to the DSL
- Do not view, copy, print, share, store or save the imagery, or ask a child to share or download.
- If you have already viewed the imagery by accident (e.g. if a young person has showed it to you before you could ask them not to), report this to the DSL (or equivalent) and seek support.
- Do not delete the imagery or ask the young person to delete it. Leave this for the DSL if needed.
- Do not ask the child/children or young person(s) who are involved in the incident to disclose information regarding the imagery. This is the responsibility of the DSL (or equivalent).
- Do not share information about the incident with other members of staff, the young person(s) it involves or their, or other, parents and/or carers.
- Do not say or do anything to blame or shame any young people involved.
- Do explain to them that you need to report it and reassure them that they will receive support and help from the DSL (or equivalent).

Child-on-child abuse

This school recognises that children sometimes display harmful behaviour themselves and that such incidents or allegations must be referred on for appropriate support and intervention.

Such abuse is unacceptable and will not be tolerated.

In the context of this policy, this abuse could for example include:

- 'upskirting'

- all forms of bullying via electronic devices

- aggravated sexting

To prevent child-on-child abuse and address the wider societal factors that can influence behaviour, the school will educate pupils about abuse, its forms and the importance of discussing any concerns and respecting others through the curriculum, assemblies and PSHE lessons.

The school will also ensure that pupils are taught about safeguarding, including online safety, as part of a broad and balanced curriculum in PSHE lessons, RSE and group sessions.

All staff will be aware that pupils of any age and sex are capable of abusing their peers and will never tolerate abuse as “banter” or “part of growing up”.

All staff will be aware that child-on-child abuse can be manifested in many ways, including sexting or cyberbullying which aims to cause emotional or psychological harm, for example.

Pupils will be made aware of how to raise concerns or make a report and how any reports will be handled – this includes the process for reporting concerns about friends or peers.

If a child has been harmed, is in immediate danger or is at risk of harm, a referral will be made to children’s social care services (CSCS).

Technology

Woodstone Community Primary School School uses a range of devices including PCs, laptops and Ipads. 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 a sophisticated content filtering system that, as far as possible, prevents unauthorized access to illegal websites and 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. Whilst filtering technology is robust and generally very effective at blocking unsuitable material in line with any other system, it is still possible for some unwanted material to occasionally get past the filters. To deal with this, staff will liaise with the school technology partner to investigate and react immediately to prevent re-occurrence.

Email Filtering – we use Office 365 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 – All school devices that hold personal data (as defined by the Data Protection Act 1998) are encrypted. No data is to leave the school on an un-encrypted device; all devices that are kept on school property and which may contain personal data are encrypted. Any breach (i.e. loss/theft of device such as laptop or USB keydrives) 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 and students will be unable to access laptops and PCs without a username and password. Staff and student passwords will change regularly or if there has been a compromise, whichever is sooner.

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 Headteacher if there are any concerns.

Safe Use

Internet – Use of the Internet in school is a privilege, not a right. Children using the internet in school will always be supervised and their internet use should be purposeful and have a clear place within the curriculum. Any child who demonstrates they are not able to use the internet safely will be denied access. Similarly, staff are welcome to use the internet for personal use during breaktime and lunchtime but their behaviour online should always reflect the safer working practice guidance.

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. All staff and Governors are provided with a work email address which should be used for all correspondence regarding school matters.

Photos and videos – Permission for use of digital media such as photos and videos is sought from parents when the pupils start at Woodstone. All parents must sign a photo/video release slip; non-return of the permission slip will not be assumed as acceptance. These are kept for reference in the school office and staff should make themselves aware of these before sharing digital media more widely.

Staff/Visitors/Governors/Volunteers/Contractors/Personal Mobile Phones and Smart Watches

All staff are reminded that personal mobile telephones should not be visible, seen or used in school except when these are used in the staffroom or in the case of an extreme emergency. Personal mobile phones must never be used for any school activity for the purpose of photographs or recording.

- All personnel must ensure that their mobile phones and recording devices are stored securely during working hours on school premises or when on outings. (This includes visitors, volunteers and students)
- Mobile phones must not be used in any teaching area in school or within any child's toilet or changing areas unless in a personal emergency
- Staff are permitted to wear Smart watches in school but should follow the same guidance as suggested for the use of mobile phones in school
- Staff and children are not permitted to wear watches with a camera function
- Under no circumstances must cameras of any kind be taken into the toilet area without prior consultation with a member of the leadership team.
- If photographs need to be taken in the toilet area, i.e. photographs of the children washing their hands, then they must be taken using the designated equipment; a member of the leadership team must be asked first and staff to be supervised whilst carrying out this kind of activity.
- Only school equipment should be used to record classroom/extended school activities and should be stored only on school devices
- Images taken on school devices must be deemed suitable without putting the child/children in any compromising positions that could cause embarrassment or distress.
- All staff are responsible for the location and secure storage of the school devices at the end of each school day.
- During school outings it is appropriate for key staff to nominate a preferred device to be used **only** for purpose of emergency contact
- All telephone contact with parents or carers must be made on the main school phone or school mobile

Pupils - Personal Mobile Phones

We recognise that mobile phones are part of everyday life for many children and that they can play an important role in helping pupils to feel safe and secure. However we also recognise that they can prove a distraction in school and can provide a means of bullying or intimidating others. Therefore:

- Pupils are not permitted to have mobile phones at school or on trips
- If in the rare event of a parent wishing for his/her child to bring a mobile phone to school to contact the parent after school:
  A) the parent must discuss the issue first with their child's teacher.

B) the phone must be handed in to the office, switched off, first thing in the morning and collected from them by the child at home time (the phone is left at the owner's own risk).

- Mobile phones brought to school without permission will be confiscated and returned at the end of the day.

Where mobile phones are used in or out of school to bully or intimidate others, then the Headteacher does have the power to intervene 'to such an extent as it is reasonable to regulate the behaviour of pupils when they are off the school site' - refer to Bullying Prevention Policy.

Gaming

The use of gaming devices is not permitted in school. Children are permitted to play games related to the curriculum on approved websites.

Social Networking – there are many social networking services available; Woodstone Community Primary 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 Woodstone Community Primary School and have been appropriately risk assessed;

- Twitter
- eSchools website.

Should staff wish to use other social media, permission must first be sought via the Headteacher for a decision to be made. Any new service will be risk assessed before use is permitted.

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 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 e-safety incident is to be brought to the immediate attention of the Headteacher. The Headteacher will assist you in taking the appropriate action to deal with the incident and to fill out appropriate paperwork.

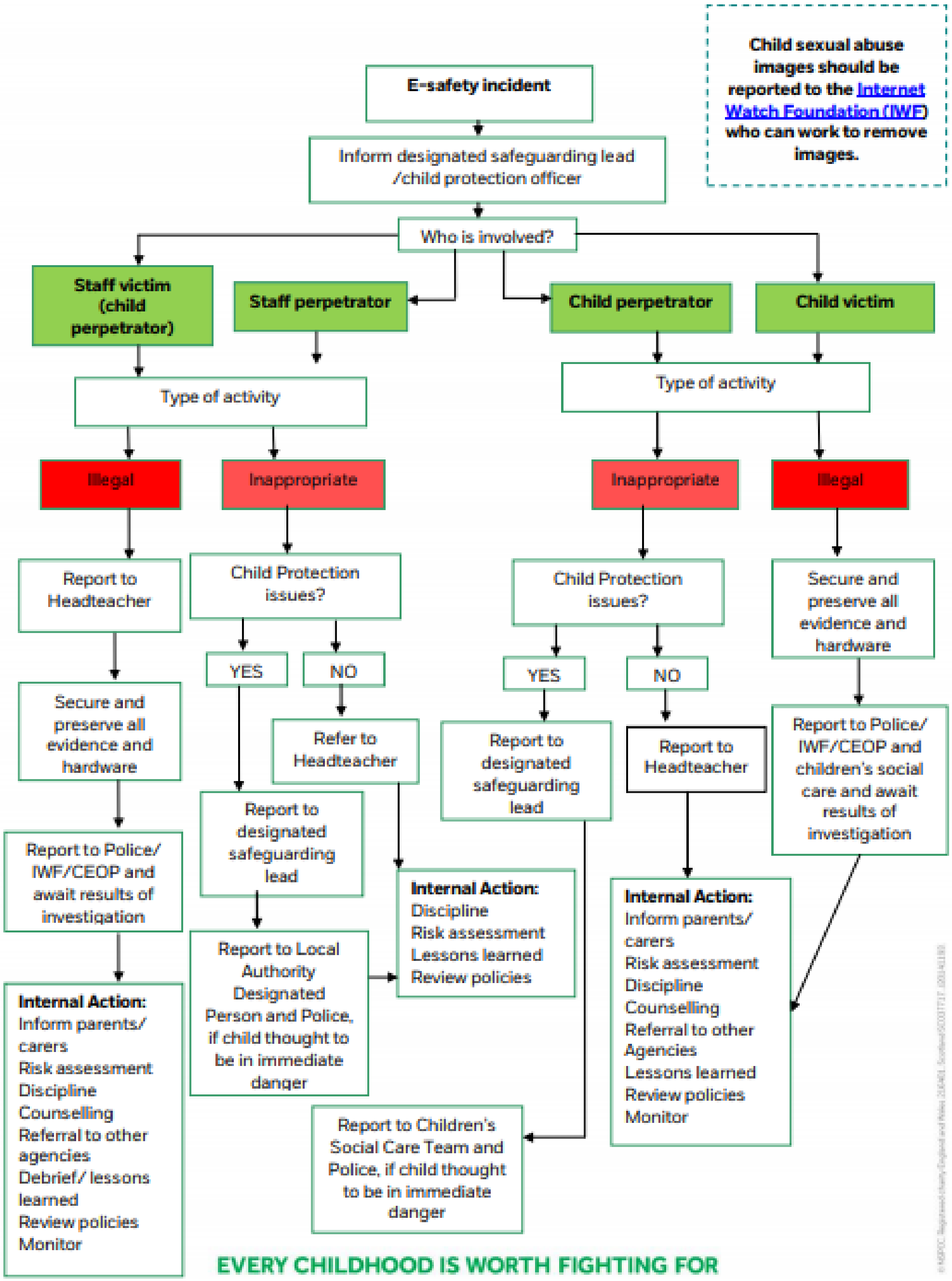
Training and Curriculum - It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. As such, Woodstone Community Primary School will have a regular programme of training which is suitable to the audience.

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 is taught through our wider Computing curriculum for which we follow Purple Mash, as well as being taught discreetly through Anti-bullying week and E-safety day.

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

The Computing co-ordinator and Headteacher are responsible for developing a programme of training and awareness for the school year. 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.

What to do if a pupil or a teacher reports an e-safety incident



Child sexual abuse images should be reported to the Internet Watch Foundation (IWF) who can work to remove images.

E-safety incident

Inform designated safeguarding lead /child protection officer

Who is involved?

Staff victim (child perpetrator)

Staff perpetrator

Child perpetrator

Child victim

Type of activity

Illegal

Report to Headteacher

Secure and preserve all evidence and hardware

Report to Police/ IWF/CEOP and await results of investigation

Internal Action:
Inform parents/ carers
Risk assessment
Discipline
Counselling
Referral to other agencies
Debrief/ lessons learned
Review policies
Monitor

Inappropriate

Child Protection issues?

YES

Report to designated safeguarding lead

Report to Local Authority Designated Person and Police, if child thought to be in immediate danger

NO

Refer to Headteacher

Internal Action:
Discipline
Risk assessment
Lessons learned
Review policies

Type of activity

Inappropriate

Child Protection issues?

YES

Report to designated safeguarding lead

Report to Children's Social Care Team and Police, if child thought to be in immediate danger

NO

Report to Headteacher

Internal Action:
Inform parents/ carers
Risk assessment
Discipline
Counselling
Referral to other Agencies
Lessons learned
Review policies
Monitor

Illegal

Secure and preserve all evidence and hardware

Report to Police/ IWF/CEOP and children's social care and await results of investigation

EVERY CHILDHOOD IS WORTH FIGHTING FOR