

POLICY NO: 8

E-SAFETY & ACCEPTABLE USE POLICY

Rationale

Peaslake Free School is committed to leverage the power of technology to enhance the teaching and learning experience in the school and to maximise the access it provides to connect with the outside world. The aim of this policy document is to safeguard the pupils, the staff and members of the school community, to provide clear advice and guidance on how to minimise risks. ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. This e-safety policy applies to all members of the school community who have access to and users of school digital systems both in and out of school.

Aim of the E-Safety Policy

- The main aim of the policy is to allow the school to take full advantage of the positive impacts of technology on teaching, learning and support
- To protect children and staff from the inappropriate use of technology which could harm the children or individual
- To establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.
- To protect the reputation of the school and all who work in it.

This policy should be read in conjunction with other School policies, particularly the Staff Acceptable Use of IT policy and Safeguarding Policy.

Peaslake Free School recognises that the use of technology has become a significant component of many safeguarding issues such as: Child Sexual Exploitation, Radicalisation, Sexual Predation and others. Therefore, Peaslake Free School educates staff and pupils to help reduce the risk of harm online by focusing on the three categorised areas of risk:

Content: being exposed to illegal, inappropriate or harmful material.

Contact: being subjected to harmful online interaction with other users.

Conduct: personal online behaviour that increases the likelihood of, or causes, harm.

Responsibilities:

The Chair of Governors:

is responsible for appointing a Safeguarding Governor, with lead responsibility for e-safety, who will:

- review this policy at least annually and as necessary in response to any e-safety incident to ensure that the policy is up to date and covers all aspects of technology use within the school.
- keep up to date with emerging risks and threats through technology use
- receive termly updates in regards to training, identified risks and any incidents
- keep the Chair of Governors and fellow Governors updated on e-safety matters
- attend the E-Safety Committee where possible
- with the Head Teacher/DSL undertake an annual review of how e-safety incidents have been dealt with and ensure the policy was effective and appropriately applied in managing those incidents

**PEASLAKE FREE SCHOOL
POLICY DOCUMENT**

Head

The Head has overall responsibility for e-safety within the school and will:

- keep up to date with emerging risks and threats through technology use
- undertake CEOP training as necessary
- have appropriate training and professional development in order to undertake the role
- ensure that all e-safety incidents are dealt with promptly and appropriately
- advise the Governors and staff on all e-safety matters
- co-ordinate responses to e-safety incidents, in consultation with Safeguarding governor
- ensure e-safety training throughout the school is planned and up to date and appropriate to the recipient: pupils, staff and governing body.
- keep up to date with the latest risks to children whilst using technology and with the latest research and available resources for school and home use, undertaking any necessary training
- keep up to date with the latest PREVENT advice linked to online safety
- engage with parents and the School community on e-safety matters at School and at home
- liaise with Surrey Safeguarding e-safety team, IT technical support and other agencies as required
- ensure staff know what to report and how to document concerns or incidents
- review this policy regularly and bring any matters of concern to the attention of the Head
- with the Safeguarding Governor, undertake an annual review of how e-safety incidents have been dealt with and ensure the policy was effective and appropriately applied in managing those incidents

Designated Safeguarding Lead

The DSL is the headteacher with e-safety responsibilities and will:

- Ensure that staff understand this policy and that it is being implemented consistently
- Will, with other staff, address any online safety issues or incidents
- Ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensure that any incidents of cyber-bullying are dealt with appropriately in line with this policy

All Staff

All staff are users of the network and have signed Acceptable Use policies which must be followed. They are also responsible for ensuring that:

- they understand all details within this policy. If anything is not understood it should be brought to the attention of the Head Teacher who is also the DSL.
- this policy is implemented consistently
- they agree and adhere to the terms on acceptable use of the schools' ICT systems and the internet.
- they understand what cyber-bullying is and respond according to the Behaviour Policy.
- any e-safety incident is reported as quickly as possible to the Head of Safeguarding, or in their absence, to a member of the Safeguarding Team.
- they seek any support, training or advice they require in this rapidly changing area from the Head Teacher/DSL
- Staff are reminded that e-safety incidents often involve Safeguarding issues; School Safeguarding procedures must be followed.

**PEASLAKE FREE SCHOOL
POLICY DOCUMENT**

Parents

Parents are expected to notify a member of staff or the headteacher:

- concerns or queries in relation to online safety.
- concerns over cyber-bullying or inappropriate uses of digital technology

Cyber-bullying is when a person or a group of people uses the internet, mobile phones, online games or any other kind of digital technology to threaten, tease, upset or humiliate someone else. (Childline 2013)

Pupils should:

- understand what cyber-bullying is
- understand that the School will not tolerate cyber-bullying and that pupils who cyber-bully, particularly when this is repeated or aggressive in nature, can expect to be suspended or expelled from School
- understand that being a 'bystander' or passing on images or messages created by cyber-bullies could itself be defined as cyber-bullying
- be aware that if investigation of an e-safety incident suggests that a pupil's misbehaviour may be criminal or pose a serious threat to a member of the public, the Head will contact the Police

When pupils have a concern or a question about how others are treating them / how a friend or another pupil is being treated / their own behaviour, they are expected to bring this promptly to the attention of a teacher or parent so that help, support and advice can be provided.

Why Do We Use the Internet?

- The purpose of internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.
- The Internet is part of the statutory curriculum and is a necessary tool for learning.
- The Internet is part of everyday life for education, business and social interaction. The school has a duty to provide students with quality internet access as part of their learning experience.

Use of the schools' internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

Teaching and Learning

Appropriate use of the Internet has proven educational benefits including raising pupil attainment. The School's Internet access is designed to enhance and extend education by allowing:

- access to worldwide resources including museums and art galleries
- access to experts in many fields for both staff and pupils
- inclusion in the National Education Network which connects all UK Schools
- professional development for staff through access to National developments, education materials and effective curriculum practice.
- staff to guide pupils onto online activities that support the learning outcomes planned for pupil's individual age and ability.
- pupils to be educated in the effective use of Internet research including knowledge retrieval, location and evaluation.
- pupils to use age-appropriate tools to research internet content

Acceptable use of The Internet, Managing Internet Access and Authorisation

- All staff will read and sign the Staff Acceptable Use of IT Policy (8B) (Appendix 1) before using any of the ICT resources
- Parents will be asked to read the Pupil Acceptable Use Policy (8A) for pupil access and discuss it with their child where appropriate
- All visitors to the site who require internet access will be asked to read the Staff Acceptable Use Policy (8B)
- Pupils will access the internet by adult demonstration to specific and approved on-line materials
- The school will take all possible precautions to ensure that users access only appropriate materials
- School ICT systems' capacity and security will be reviewed regularly
- Virus protection will be updated regularly
- All members of the school community will be informed about the procedure for reporting e-safety concerns including: breaches of filtering, cyber bullying, illegal content etc.

Filtering

The School will ensure systems to protect pupils are reviewed and improved and that the filtering methods selected are appropriate, effective and reasonable. If staff or pupils come across unsuitable on-line materials, the site must be reported to Headteacher.

The school uses: 'SafeDNS home' configured to block all inappropriate content.

Staff Using Devices outside School

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate Staff Acceptable Use of IT Policy (8B) (Appendix 1).

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school.

Any USB devices containing data relating to Peaslake Free School must be encrypted. If staff have any concerns over the security of their device, they must seek advice.

Email

Email is an essential means of communication for staff. Directed email can bring significant educational benefits, interesting projects between schools in neighbouring villages and different continents.

- Pupils can only use approved school email accounts with teacher supervision for school purposes
- Pupils must not reveal personal details of themselves or others in email communication
- Staff should not use personal email accounts for school use.

The School Website and Publishing Pupils Work

The School Website promotes the school, publishes pupils' work to celebrate it and publishes resources for topics. Publication of any material online should be considered from a personal and school security viewpoint.

- The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- Photographs of pupils will be carefully selected, and material will be provided that cannot be reused.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before images are electronically published.
- The School has a policy regarding the use of images of children which outlines procedures.

Reporting and Responding

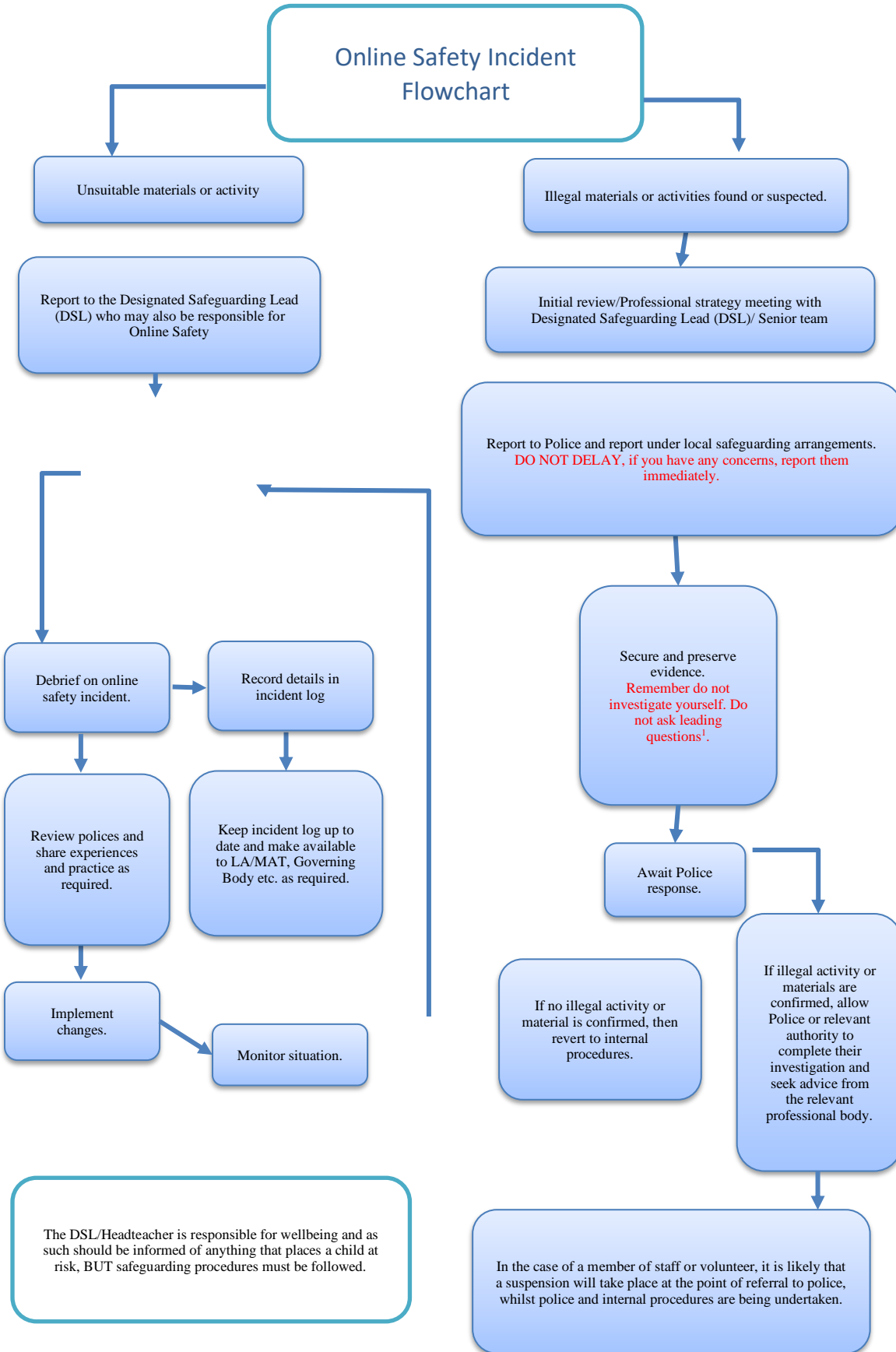
The school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

- there are clear reporting routes (see flowchart below) which are understood and followed by all members of the school community. These are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.
- all members of the school community will be made aware of the need to report online safety issues/incidents.
- reports will be dealt with as soon as is practically possible once they are received.
- the Designated Safeguarding Lead, Online Safety Lead and other responsible staff have appropriate skills and training to deal with online safety risks.

**PEASLAKE FREE SCHOOL
POLICY DOCUMENT**

**PEASLAKE FREE SCHOOL
POLICY DOCUMENT**

**Online Safety Incident
Flowchart**



The DSL/Headteacher is responsible for wellbeing and as such should be informed of anything that places a child at risk, BUT safeguarding procedures must be followed.

In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

**PEASLAKE FREE SCHOOL
POLICY DOCUMENT**

**PEASLAKE FREE SCHOOL
POLICY DOCUMENT**

Assessing Risk

Peaslake Free School will take all reasonable precautions to ensure that users access only appropriate material. The school filtering and monitoring provision is agreed by senior leaders, governors, and the IT service provider. It is regularly reviewed (at least annually) and updated in response to change in technology and patterns of e-safety incidents and behaviours. There are established and effective routes for users to report inappropriate content. However, we recognise that due to the international scale and linked nature of Internet content, no system can be 100% effective and so it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access.

Policy Ratified by the Governors: (Head update September 2023)

Review date: Annually

Appendix 1

POLICY NO: 8 (B)

STAFF ACCEPTABLE USE OF IT POLICY

Rationale

The Peaslake Free School Acceptable Use Policy sets out guidelines for the appropriate use of technology within Peaslake Free School. We recognise the importance of ICT in education and the needs of staff and pupils to access the computing facilities available within the school.

All staff, and visitors who use school ICT facilities are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Principal.

Aims of Acceptable Use Policy

- To protect pupils, staff and parents
- To ensure professional integrity is not compromised
- To ensure the setting is not brought into disrepute
- To make ICT resources available for pupils to use in their learning.

The AUP will be revised annually. Before signing, the AUP should be read carefully to ensure that the conditions of use are accepted and understood.

School Strategy:

The school employs a number of strategies in order to maximise learning opportunities and reduce risks associated with the Internet:

- Internet sessions are always supervised by a teacher
- Two levels of filtering are used in order to minimise the risk of exposure to inappropriate material
- Teachers and pupils will be provided with training in the area of internet safety
- Virus protection software is present on all machines and is updated and checked automatically on a daily basis
- Children are taught about safe internet use by their teachers.

Policy Commitment

All staff and visitors who work within the school are expected to sign the attached commitment form for the Acceptable Use of IT Policy.

Policy Ratified by the Governors:

Review date:

ATTACHMENT ONE

Staff Policy Commitment

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Principal
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role
- I will not give out my own personal details, such as mobile phone number and personal e-mail address, to pupils
- I will only use the approved, secure e-mail system(s) for any school business
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Headteacher. Personal or sensitive data taken off site must be encrypted
- I will not install any hardware or software without permission of the Headteacher/DSL.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes inline with school policy and with written consent of the parent, carer or staff member
- I understand that all my use of the Internet and other related technologies can be monitored and logged
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community
- I will respect copyright and intellectual property rights
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute
- I will support and promote the school's e-Safety policies and help pupils to be safe and responsible in their use of ICT and related technologies.
- I will not use my mobile phone on the school premises during the school day.
- I understand this forms part of the terms and conditions set out in my contract of employment.

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school

Signature:

Date: