Online Safety Policy

Date of document:	October 2021
Date for review:	October 2023
Lead reviewer:	Greg McGill
Approval by:	Governing body (S Carter)

This policy applies to all members of the school (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.
The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate online safety behaviour that take place out of school.

The finalised version of **Keeping Children Safe in Education 2021** also introduced a new area of online safety risk: commerce. This area sits alongside the existing risk areas of content, contact and conduct. Commerce includes risks such as online gambling, inappropriate advertising, phishing and financial scams.

Policy Statement

Safeguarding is a serious matter: at Swallowfield Lower School we use technology and the internet extensively across all areas of the curriculum. Online safeguarding 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:

1. To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.
2. 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.

Roles and Responsibilities

Governing Body
The governing body is accountable for ensuring that out school has effective policies and procedures in place. As such they will:

- Review this policy every two years 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 these incidents.
- Appoint one governor **(Sylvia Carter)** who has overall responsibility for the governance of online safety at the school who will:
    - Keep up to date with the emerging risks and threats through technology use
    - Receive regular updates from the head teacher in regards to training, identified risks and any incidents.
    - Report to governors on online safety issues that arise

Head teacher and Senior Leaders
Reporting to the governing body, the head teacher has overall responsibility for online safety within our school.

The Head teacher will ensure that:

- Online safety training throughout the school is planned and up to date and appropriate to the recipient, e.g. pupils, all staff, SLT and governing body, parents.
- The designated online safety lead (Sam Hayler) has had appropriate CPD in order to undertake the day to day duties.
- The Headteacher and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- All online safety incidents are dealt with promptly and appropriately. The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents later in this policy)
- The Senior Leadership Team will receive regular monitoring reports from the Online safety Co-ordinator.

Online safety Lead
The day to day duty of online safety officer is devolved to: **Sam Hayler**
The online safety officer will:

- Keep up to date with the latest risks to children whilst using technology; familiarise herself with the latest research and available resources for school and home use.
- Take day to day responsibility for online safety issues and has a leading role in establishing and reviewing this policy regularly along with other related document and bring any matters to the attention of the Head teacher.
- Advise the Head teacher, governing body on all online safety matters.
- Meets with the online safety governor regularly meets regularly to discuss current issues, review incident logs.
- Provides training and advice for staff and ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- Retain responsibility for the online safety incident log, ensure staff know what to report and ensure the appropriate audit trail as well as a log of incidents to inform future online safety developments.

- Support the SLT in writing an Online Safety Review in line with Keeping Children safe in Education 2021.
    -This review should be supported by an annual risk assessment that considers and reflects the risks their pupils face.
- Engage with parents and the school community on online safety matters at school and/or home.
- Liaise with IT technical support and other agencies as required.
- Ensure any technical online safety measures in school (e.g. internet filtering software, behaviour management software) are fit for purpose.
- Make herself aware of any reporting function with technical online safety measures, i.e. internet filtering reporting function, liaise with the Head teacher and responsible governor to decide on what reports may be appropriate for viewing.
- Reports regularly to the Senior Leadership Team and in partnership with them decides on the investigation/ action and sanctions process for any online safety incidents.
- That the use of the network / internet/ email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher and/ or Online safety Lead for investigation / action / sanction

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 systems) updates are regularly monitored and devices updated as appropriate.
- Any online 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 online safety officer and the Head teacher.
- Passwords may not be applied to shared pupil areas. Passwords for staff will be a minimum of 6 characters.
- Machines are encrypted and memory sticks containing pupil information are encrypted.
- The school meets required online safety technical requirements and any Local Authority / other relevant body Online safety Policy / Guidance that may apply.
- That they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- That monitoring systems are implemented and updated as agreed in school policies.

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 head teacher or online safety officer.
- They have an up to date awareness of online safety matters and the current school policy and practices.
- They have read, understood, signed and abide by the acceptable use policy**.**
- All digital communication with pupils and parents/ carers should be on a professional level and only carried out using official school systems.
- Online safety issues are embedded in all aspects of the curriculum and other activities and implement current policies with regard to the use of digital technologies, mobile devices, cameras etc in lessons.
- Pupils understand and follow the online safety and acceptable use policies.

- In lessons where internet use is pre-planned students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Any online safety incident is to be reported to the online safety lead, and/ or the head teacher and recorded in an online safety incident log.

Parents and Carers
Parents play the most important role in the development of their children; as such the school will offer the parents the skills and knowledge they need to ensure online safety of children outside the school environment. Through parent meetings, school newsletters, regular promotion and links on our website, the school will keep parents up-to-date with new and emerging online 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 sign the student acceptable use policy to show support of the policies and procedures before any access can be granted to school ICT equipment or services.

Education - All Pupils
Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

• A planned online safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited.
• Key online safety messages should be reinforced as part of a planned programme of assemblies.
• Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
• Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
• Pupils should be helped to understand the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
• Staff should act as good role models in their use of digital technologies the internet and mobile devices.
• In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Technology
Swallowfield Lower School uses a range of devices including I pads, Cameras, PCs, kindles and Laptops. The school will be responsible for ensuring that the school network is as safe and secure as reasonable possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities.

In order to safeguard the pupil and in order to prevent loss of personal data we employ the following:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.

- Servers, wireless systems and cabling are securely located and physical access restricted
- Group and class log-ons are used for children in the school as they are age appropriate but the school is aware of the risks associated with not being able to identify any individual who may have infringed the rules set out in the policy. To address this, pupils should always be supervised and members of staff should never use a class log on for their own network / internet access.
- The administrator password for the school, used by the IT technical team is also available for the Headteacher and is kept in a locked filing cabinet in the school office.
- The school Business Manager and IT technical support are responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users. We use an educational filtered system that prevents unauthorized access to illegal websites. Content lists are regularly updated and internet use is logged and regularly monitored. 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 co-ordinator, 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 head teacher.
- Passwords: All staff will be unable to access a device that can access personal or confidential data without a unique username and password. The ICT co-ordinator and IT support are responsible for ensuring that these are kept secure.
- 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 head teacher 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 this online safety and the staff acceptable use policy; pupils (or their parents) upon signing and returning their acceptance of the acceptable use policy.

Email: All staff are reminded that their 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 emails for work purposes are not permitted.

Social Media - Protecting Professional Identity
All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

School staff should ensure that:

- No reference should be made in social media to students / pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

PREVENT

In accordance with the Prevent Strategy, which aims to prevent children and young people being exposed to extremist views and at risk of radicalisation, staff are all trained on the channel programme
https://educateagainsthate.com/what-is-channel/
https://www.gov.uk/government/case-studies/the-channel-programme

This responsibility extends to online safety and protecting children from extremist material online. Through this training, staff are aware of how the internet is used to radicalise people. Filtering should prevent access to such extremist sites but any material accessed at school should be treated as an online safety incident and dealt with accordingly. Disclosures or concerns regarding exposure outside of school should be treated as a safeguarding incident and dealt with in accordance with the Safeguarding policy and procedures (Safeguarding policy).
Parents and carers are informed about the risks of radicalisation and extremism via online safety newsletters and The Prevent Action Plan.