Saxon Hill Academy

ONLINE SAFETY POLICY

Issue Date: October 2018

Date of review: October 2019

Chair of Governors: Richard Metcalfe

Background / Rationale

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil / student achievement. However, the use of these new technologies can put young people at risk within and outside the school.

Some of the dangers they may face include:

• Access to illegal, harmful or inappropriate images or other content

• Un-authorised access to / loss of / sharing of personal information

• The risk of being subject to grooming by those with whom they make contact on the internet.

• The sharing / distribution of personal images without an individual's consent or knowledge

• Inappropriate communication / contact with others, including strangers

• Cyber-bullying

• Access to unsuitable video / internet games

• The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this Online Safety policy is used in conjunction with other school policies (e.g. behaviour, anti-bullying and child protection policies). As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to

which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

Development and Monitoring

Role - Named Person

IT Manager and Assistant: Dave Orum and Michelle Rowberry

Designated Safeguarding Lead and Deputies: Kim Thomas, Helen Bowers and Mel Newbury

This Online Safety policy has been developed by the Designated Safeguarding Team and Senior Leaders. As part of this policy, records will be maintained of Online Safety related incidents involving staff and pupils and any incidents recorded will be treated in accordance with our safeguarding procedures. This policy will be reviewed at least annually.

Should serious online safety incidents take place, the following external persons / agencies should be informed:

Staffordshire Police (Reporting Cyber Crime, if criminal activity has occurred) https://www.staffordshire.police.uk/Report

For information and guidance and to report to CEOP https://www.ceop.police.uk/safety-centre/

The school will monitor the impact of the policy using:

- Feedback from staff, pupils, parents / carers, governors
- Logs of reported incidents
- Internet activity monitoring logs

Scope of the Policy

This policy applies to all members of the school community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school. The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils 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 out of school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the search for and of

electronic devices and the deletion of data. The school will deal with such incidents within this policy and associated behaviour policy and will, where known, inform parents / carers of incidents of inappropriate online safety behaviour that take place out of school.

Roles and Responsibilities

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy.

Headteacher / Senior Leaders

• The Headteacher is responsible for ensuring the safety (including Online safety) of members of the school community, though the day to day responsibility for Online safety will be delegated to the Designated Safeguarding Lead and Deputies.

• The Headteacher is responsible for the implementation and effectiveness of this policy. They are also responsible for reporting to the Governing Body, the effectiveness of the policy and, if necessary, make any necessary recommendations re further improvement.

• The Headteacher / Senior Leaders are responsible for ensuring that the Designated Safeguarding Lead, Deputies and other relevant staff receive suitable CPD to enable them to carry out their online safety roles.

• The Headteacher / 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.

• The Headteacher and 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 Whistleblowing and Safeguarding Policy)

Designated Safeguarding Lead and Deputies

The Designated Safeguarding Lead and Deputies:

• Take day to day responsibility for online safety issues and have a leading role in establishing and reviewing the school online safety policies / documents

• Ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place

• Reports to the School Leadership Team serious breaches of the Online Safety Policy

• Provides training and advice for staff

• Liaise with the Local Authority

• Receive reports of online safety incidents and create a log of incidents to inform future online safety developments

Teaching and Support Staff

Teaching and Support Staff are responsible for ensuring that:

• They have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices

• They have read and understood the Online Safety Policy, school Staff Acceptable Use Policy / Agreement (AUP)

• They report any suspected misuse or problem to the Designated Safeguarding Lead or Deputies for investigation / action / sanction

• Digital communications with pupils and parents / carers (email / voice) should be on a professional level

• Students / pupils understand and follow, as appropriate for age and ability, the school Online Safety and Acceptable Use Policy

• Students / pupils understand and follow online safety rules and they know that if these are not adhered to, sanctions will be implemented in line with our Behaviour and Anti-Bullying policies.

• In lessons where internet use is 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.

Designated Safeguarding Lead and Deputies should be trained in Online safety issues and be aware of the potential for serious child protection issues to arise from:

• Sharing of personal data

• Access to illegal / inappropriate materials

• Inappropriate on-line contact with adults / strangers

• Potential or actual incidents of grooming

• Cyber-bullying

• Sexting

• Revenge pornography

• Radicalisation (extreme views)

• CSE

Pupils

• Are responsible for using the school ICT systems in accordance with the Student / Pupil Acceptable Use Policy, which they will be expected to agree to before being given access to school systems, where appropriate for age and ability.

• Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so, where appropriate for age and ability.

• Will be expected to follow school rules relating to this policy e.g. safe use of cameras, cyberbullying etc.

• Should understand that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school, where appropriate for age and ability.

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than some of their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, letters, website / local online safety campaigns / literature.

Parents and carers will be responsible for:

• Endorsing (by signature) the Student / Pupil Acceptable Use Policy

• Accessing the school website / online pupil records in accordance with the relevant school Acceptable Use Policy.

Parents / carers should understand that school has a duty of care to all pupils. The misuse of non-school provided systems, out of hours, will be investigated by the school in line with our AUP, Behaviour, Anti-Bullying and Safeguarding policies.

Policy Statements - Education

Pupils Online Safety education will be provided in the following ways, as appropriate to pupils' age and ability:

• A planned Online Safety programme should be provided as part of Computing/ PHSE / other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school.

• Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities

• Students / pupils should be encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school

• Students / pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

• Students / pupils are taught the importance of keeping information such as their password safe and secure.

• Acceptable Use Policy rules for the use of ICT systems / internet will be made available for pupils to read or have read to them where appropriate to age and ability.

• Staff should act as good role models in their use of ICT, the internet and mobile devices

Education – Parents and Carers

Some parents and carers have a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's online experiences. Parents may either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report). The school will therefore seek to provide information and awareness to parents and carers through:

• Letters, web site

• Parents evenings

• Reference to external Online Safety websites

• High profile events such as Internet safety day

• Family learning opportunities

Education and Training – Staff

It is essential that all staff receive Online Safety training and understand their responsibilities, as outlined in this policy.

Training will be offered as follows:

• A planned programme of formal Online Safety training will be made available to staff. An audit of the online safety training needs of all staff will be carried out regularly.

• All new staff should receive Online Safety training as part of their induction programme, ensuring that they fully understand and agree to adhere to the school Online Safety Policy and Acceptable Use Policy • The DSL and Deputies will provide advice / guidance / training to individuals as required.

Technical – Infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably 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:

• School ICT systems will be managed through the managed service provider, in ways that ensure that the school meets the online safety technical requirements for Staffordshire Local Authority and the Shaw Education Trust

• Servers, wireless systems and cabling must be securely located and physical access restricted

• All users will have clearly defined access rights to school ICT systems

• Staff will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security

• The school maintains and supports the managed filtering service provided by Future Digital. Any incidents or activities regarding filtering will be handled by the DSL and Deputies according to the Safeguarding Policy and this Online Safety Policy.

• Appropriate security measures are in place, provided by the managed service provider, to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data

• Guest access to the school network will be authorised by the IT Support Team through the provision of limited access guest accounts which do not give access to personal information about pupils or staff.

• The school infrastructure and individual workstations are protected by up to date anti-virus software

• Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured in accordance with the SET Data Protection Policy.

Curriculum

Online Safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages in the use of ICT across the curriculum.

• Good online safety practice is an integral part of the school Computing curriculum and will be taught to pupils as part of their ICT learning.

• Where students / pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit in case the filtering has been somehow breached.

• It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked or flagged up by the monitoring software. In such a situation, staff can inform the Deputy DSL in advance of the period of study. Resulting reports, should be auditable, with clear reasons for the need for their appearance on the report.

Use of digital photographs and video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students / pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

• Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the storing, sharing, distribution and publication of those images. Those images should only be taken on school equipment. The personal equipment of staff should not be used for such purposes.

• Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

• Students / pupils must not take, use, share, publish or distribute images of others without their permission

• Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such images.

• Students' / Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

• Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website or on the school's social media.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. More detailed guidance on the collection, handling and storage of personal data can be found in the SET Data Protection Policy.

Communications

When using communication technologies the school considers the following as good practice:

• The official school email service may be regarded as safe and secure. Pupils should therefore not use other email systems when in school, or on school systems.

• Users need to be aware that email communications may be monitored.

• Users must immediately report, to the DSL or Deputies – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.

• Any digital communication between staff and students or parents / carers must be professional in tone and content and be via official used systems.

• Whole class or group email addresses may be provided to classes for educational use. Individual email addresses will be provided to some pupils if deemed appropriate for their level of ability by their class teacher.

• Students / pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.

• Personal information should not be placed on the school website on public facing calendars and only official school emails should be identified within it.

• The school allows staff to bring in their own personal devices, including mobile phones, for their own use. These need to be stored away safely from children and young people during the times when member of staff is on duty. Under no circumstances should a member of staff use their personal devices including mobile phones, to contact a pupil, parent/carer or to photograph children.

Responding to incidents of misuse

There may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse by pupils, staff or any other user appears to involve illegal activity i.e.

• Child sexual abuse images

• Adult material which potentially breaches the Obscene Publications Act

• Criminally racist material

• Other criminal conduct, activity or materials

The incident should be following in accordance with the Safeguarding Policy and if necessary, the police should also be informed.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner.

Guidelines for the use of communication technologies within school

	Staff & other adults				Students / Pupils (6 = 6TH Form Only)			
Communication Technologies	Allowed	Allowed in designated areas	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	Y						6	Y
Use of mobile phones in lessons		Y offsite in emergency					6	Y
Use of mobile phones in social time		Y					6	Y
Taking photos on mobile phones or personal camera devices				Y				Y
Use of personal tablets		Y					Y	
Use of personal email addresses in school, or on school network during own time		Y					6	Y
Use of school email for personal emails				Y				Y
Use of chat rooms / facilities				Y				Y
Use of instant messaging		Y					6	Y
Use of social networking sites				Y			6	Y
Use of personal blogs				Y			Y	
Use of educational blogs							Y	

Related Documents

Saxon Hill Academy Acceptable Use Policies

Saxon Hill Academy SET Data Protection Policy.

Saxon Hill Academy Child Protection Policy

Saxon Hill Academy Behaviour Policy

Saxon Hill Academy Anti-bullying Policy