E-Safety Policy

Status	Non Statutory	**Date created**	July 2018
Any other statutory names for this policy (where applicable)		**Date first approved**	September 2018
Responsibility for this policy (job title)	Deputy Headteacher	**Date last reviewed**	December 2019
Governors' Committee with responsibility for its review	Teaching & Learning	**Frequency of review**	Every three years
Tick here if Bucks Policy attached in its entirety		**To be put on the school website?**	Yes
Approval necessary	Sub Committee		

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff

- Relationships and sex education
- Searching, screening and confiscation.

It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on students' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The Safeguarding governor will discuss online safety as part of half-termly safeguarding meetings with the designated safeguarding lead (DSL).

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on the School's acceptable use policy.

3.2 The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead

Details of the school's DSL and DSLTeam are set out in our child protection and safeguarding policy as well relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, IT support team and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged on Safeguard and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged on Safeguard and dealt with appropriately in line with the School's behaviour and exclusion policy
- Updating and delivering staff training on online safety

- Liaising with other agencies and/or external services if necessary.

3.4 The IT Support Team

The IT Support Team and Director of Support Staff are responsible for:

- Maintaining appropriate filtering and monitoring systems to keep students safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's IT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly

3.5 All staff and volunteers

All staff and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's IT systems and the internet, and ensuring that students follow the school's terms on acceptable use
- Working with the DSL to ensure that any online safety incidents are logged on Safeguard or on an enote and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour and exclusion policy and are shared with the DSL

3.6 Parents/Carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their daughter has read, understood and agreed to the terms on acceptable use of the school's IT systems and internet.

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? - UK Safer Internet Centre
- Hot topics - Childnet International
- Parent factsheet - Childnet International.

3.7 Visitors and members of the community

Visitors and members of the community who use the school's IT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

4. Educating students about online safety

Students will be taught about online safety as part of Learning for Life and Computing:

In **Key Stage 3**, students will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns
- Understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- Report a range of concerns.

We aim to ensure that they will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours.

The school will use assemblies and form time to raise students' awareness of the dangers that can be encountered online and may also invite speakers to talk to students about this.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or via Newsletters, and in information via our website. Awareness raising sessions will be held at school from time to time to offer further guidance to parents/carers. This policy will also be shared with parents and be made available on our website.

If parents have any queries or concerns in relation to online safety including this policy, these should be raised in the first instance with the headteacher and/or the DSL.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. See the school behaviour and exclusions policy and Anti-Bullying Strategy.

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Form tutors and Heads of Year will discuss cyber-bullying with their tutor groups, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes Learning for Life and Computing.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support students, as part of safeguarding training

The school also invites parents/carers into school to hear information from external specialist speakers, in addition to sharing information on cyber-bullying via the newsletter. We are keen that parents are aware of the signs of cyber-bullying, how to report it and how they can support young people who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the anti-bullying strategy. Where illegal, inappropriate or harmful material has been spread among students, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on students' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules.

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police.

Any searching of students will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on students' electronic devices will be dealt with through the school complaints procedure.

7. Acceptable use of the internet in school

All students, parents, expected to sign an agreement regarding the acceptable use of the school's IT systems. Staff, volunteers and Governors must comply with their Code of Conduct which details acceptable use of IT equipment and systems.

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

We will monitor the websites visited by students, staff, volunteers, governors and visitors (where relevant) on a daily basis. An automated report is sent to the DSL every day of the week, including weekends and school holidays, to ensure they comply with the above.

More information is set out in the acceptable use agreements.

8. Students using mobile devices in school

Students may bring mobile devices into school, but are not permitted to use them during lessons and form time (unless given permission by teaching staff).

Any use of mobile devices in school by students must be in line with the acceptable use agreement.

Any breach of the acceptable use agreement by a student may result in the confiscation of their device or other action in line with the behaviour and exclusion policy.

9. Staff using work 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 the school's terms of acceptable use.

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 sensitive or personal data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the IT Support Team or the Director of Support Staff.

10. How the school will respond to issues of misuse

Where a student misuses the school's IT systems or internet, we will follow the procedures set out in the behaviour and exclusions policy and terms of our acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's IT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will report incidents which involve illegal activity or content to the police, and may report otherwise serious incidents.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, staff bulletin, newsletters and staff meetings).

The DSL and the DSL Team will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety on Safeguard.

This policy will be reviewed every three years by the Teaching & Learning Committee. At every review, the policy will be shared with the governing board.

13. Links with other documentation

This Online Safety Policy is linked to our:

- Child Protection and Safeguarding Policy
- Behaviour and Exclusions Policy
- Anti-Bullying Strategy
- Whistleblowing Policy
- Confidentiality and Data Protection Policy and privacy notices
- Acceptable Use Policy

Appendix

- Acceptable Use Policy for Chromebook Users
- Acceptable Use Policy for BYOD