Sherwood Primary School
Online Safety Policy

October 2020

Online Safety Policy and Pupil Acceptable Use Agreements

Context

Pupils at Sherwood Primary School have access to a range of online materials that enrich and extend teaching and learning opportunities. The benefits to teaching and learning are many and varied. Pupils will be given clear objectives for Internet use and will access material under guidance from their class teacher. Teachers will supervise pupils and take all reasonable precautions to ensure that users only access material appropriate to their learning.

Sherwood pupils are taught to use technology safely and respectfully, keeping personal information private. Pupils are taught to identify where to go for help and support, and when they have concerns about content or contact on the internet or other online technologies.

Remote Learning

We are committed to supporting our pupils in accessing learning content online from home and see online material as a key element of our approach to blended learning in light of the Coronavirus Pandemic. Please see our Remote Learning Policy.

In order to safeguard our children and teachers, a safe, robust, online platform will be used to enhance children's learning, whilst providing the highest degree possible of safety, appropriate to the age of our children. At Sherwood Primary School, our School Website will be fully utilized alongside the online platform: SeeSaw.

Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, 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

Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and 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. The policy also takes into account the National Curriculum computing programmes of study.

Roles and responsibilities

The Governing Body has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation. The governing body will co-ordinate regular meetings with appropriate staff to discuss online safety. The Governing Body will monitor online safety through minutes of the Safeguarding Team, Filtering reports and discussion with the Online Safety Champion/Designated Safeguarding Lead (DSL).

The governor who oversees online safety is Mr M Barnes.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet

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

Details of the school's designated safeguarding lead (DSL) are set out in our child protection and safeguarding policy. 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 and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board

The Online Safety Leader and Technician are responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged 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 policy

All staff, including contractors and agency 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 ICT systems and the internet and ensuring that pupils follow the school's terms on acceptable use
- Working with the DSL to ensure that any online safety incidents are logged 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 policy

Parents are expected to:

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

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

UK Safer Internet Centre: https://www.saferinternet.org.uk/advicecentre/parents-and-carers/what-are-issues

Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics

Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy and expected to read and follow it. They will be expected to agree to the terms on acceptable use. A wi-fi code is available for visitors to use if required as part of this visit. This code is changed regularly and is not available to staff or parents.

Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum. The Sherwood Primary School Curriculum outlines the content for our Digital Literacy and Citizenship Curriculum.

Educating parents about online safety

We believe in working closely with our parents to support pupils in developing safe practice when using online technology and therefore provide regular updates through our newsletters, assemblies and class web pages.

This policy will also be shared with parents. Online safety will also be covered during parents' evenings. If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL. Concerns or queries about this policy can be raised with any member of staff or the headteacher.

Cyber-bullying

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 also the school behaviour policy.)

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils 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 pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their class and the issue will be addressed in assemblies. Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyberbullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding. The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected. In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, 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.

Examining electronic devices

Pupils at Sherwood Primary School are not permitted to bring mobile phones or other devices into school unless there are exceptional circumstances. In these circumstances, mobile phones are stored securely by the class teacher. 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 pupils' 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
- Disrupt teaching
- 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
- Retain it as evidence (of a criminal offence or a breach of school discipline)
- Report it to the police

Any searching of pupils 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 pupils' electronic devices will be dealt with through the school complaints procedure.

Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 and 2). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant. 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 pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above. More information is set out in the acceptable use agreements in appendices 1 and 2.

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. Staff must use Office 365 to save work that may contain any pupil data. If staff have any concerns over the security of their device, they must seek advice from the Headteacher.

How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in the behaviour policy. 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 ICT 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 disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident. The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

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, e-bulletins and staff meetings). The DSL 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. More information about safeguarding training is set out in our child protection and safeguarding policy.

Monitoring and Filtering

Sherwood Primary School uses **Surf Protect from Exa Network** to filter inappropriate content from users in school. We also monitor online activity of staff, children and visitors to Sherwood Primary School. Any concerns that arise are reported immediately to our Designated Safeguarding Leader and Online Safety Lead (Mr P Whelan).

A report is also generated on a weekly basis and reviewed by the Headteacher and Online Safety Leader. Action is taken immediately to address any concerns that arise (in line with our Behaviour, Anti-Bullying, Equalities, Safeguarding or PREVENT policies and procedures). This information is then shared on a termly basis with the Safeguarding Team (a sub-committee of our Senior Leadership team). Any action that arises from this is reported to the Governing Body.

This policy will be reviewed by the Health, Safety and Safeguarding Committee. At every review, the policy will be shared with the full governing board.

Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure

Approval date: October 2020

Review date: October 2022

Signed (Headteacher):

Signed (On behalf of the Governing Body):

Pupil Acceptable Use Agreement

Foundation Stage and Key Stage 1 (Year 1 and 2)

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers / tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of the computer and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen

Pupil Acceptable Use Agreement

Key Stage 2 (Years 3-6)

I understand that I must use Sherwood systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:

- I understand that Sherwood School will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc)
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that Sherwood School devices are for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try to download or upload anything from the internet.
- I will not use Sherwood School systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg YouTube).

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security of the technology it offers me and to ensure the smooth running of the *school*:

- I will not bring my own personal devices (mobile phones / USB devices etc) into school.
- I will immediately report any damage or faults involving equipment or software, however this may have happened
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings
- I will not use social media sites in school

When using the internet for research, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that Sherwood School also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I may no longer be allowed to access the school network and internet.
- I understand that Sherwood School will contact my parents if I fail to comply with this Acceptable Use Agreement.

Name of Pupil: .....

Class: .....

Signed: .....

Date: .....