Title	Online Safety Policy ***Includes Acceptable Use Policy (AUP)***
Year	2020/2021
Author	Jane Page, Senior Vice Principal
Date approved by Full Governing Body	September 2020 / **Revised January 2021**
Review Date	January 2022

Contents

1. Aims 3
2. Legislation and guidance 3
3. Roles and responsibilities 3
4. Educating learners about online safety 4
5. Educating parents about online safety 6
6. Cyber-bullying 6
7. Acceptable use of the internet in school 7
8. Learners using mobile devices in school 7
9. Staff using work devices outside school 7
10. How the school will respond to issues of misuse 7
11. Training 7
12. Monitoring arrangements 7
13. Links with other policies 8
Appendix 1: Acceptable use policy agreement (AUP) 9

1. Aims

Our school aims to:

- ✓Have robust processes in place to ensure the online safety of learners, 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, 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 learners' 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 Body

The Governing Body has overall responsibility for monitoring this policy and holding the Principal to account for its implementation.

The Safeguarding Governor will meet with the DSL to discuss online safety. All governors should ensure they have read and understood this policy.

3.2 The Principal

The Principal is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school. All staff will be required to sign that they have read and understood this policy through the school's online safety programme, My Concern. This will be monitored by the DSL.

3.3 The Designated Safeguarding Lead

Details of the school's DSL and deputies are set out in our Child Protection and Safeguarding Policy.

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

- ✓ Supporting the Principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the school;
- ✓ Working with the Principal, ICT lead and other staff, as necessary, to address any online safety issues or incidents;
- ✓ Ensuring that any online safety incidents are logged using My Concern and dealt with appropriately;
- ✓ Updating and delivering staff training on online safety;
- ✓ Liaising with other agencies and/or external services if necessary;

3.4 ICT Provider and ICT Lead

Our ICT provider is Dataspire, Dataspire will work under the direction of the school's ICT Lead. The ICT lead for Wootton Park school is Kayleigh Smith. Dataspire, in conjunction with the ICT Lead, are responsible for:

- ✓Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep learners 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 sent to the DSL.
- ✓Ensuring that any incidents of cyber-bullying sent to the DSL.

3.5 All staff

All staff are responsible for:

- ✓Maintaining an understanding of this policy;
- ✓Implementing this policy consistently;
- ✓Agreeing and adhering to the terms in the staff ICT Acceptable Use Policy (APU), Appendix 1.
- ✓ Ensuring that learners follow the school's terms as outlined in the Learner ICT Acceptable Use Policy (APU), Appendix 1.
- ✓Working with the DSL to ensure that any online safety incidents are logged on My Concern 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.

3.6 Parents

Parents are expected to:

- ✓ Notify a member of staff or the Principal of any concerns or queries regarding this policy;

  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

There is also an online safety section for parents/carers on our school website.

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT 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 Listed in the Staff Acceptable Use Policy.

4. Educating learners about online safety

Learners will be taught about online safety as part of the curriculum. This is in line with the 2020 documentation outlined below:

- ✓Relationships education and health education in primary schools
- ✓Relationships and sex education and health education in secondary schools

In **Key Stage 1**, learners will be taught to:

- ✓ Use technology safely and respectfully, keeping personal information private;

- ✓ Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

Learners in **Key Stage 2** will be taught to:

- ✓ Use technology safely, respectfully and responsibly;
- ✓ Recognise acceptable and unacceptable behaviour;
- ✓ Identify a range of ways to report concerns about content and contact.

By the **end of primary school**, learners will know:

- ✓ That people sometimes behave differently online, including by pretending to be someone they are not;
- ✓ That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous;
- ✓ The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them;
- ✓ How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met;
- ✓ How information and data is shared and used online;
- ✓ How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.

In **Key Stage 3**, learners 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.

Learners in **Key Stage 4** will be taught:

- ✓ To understand how changes in technology affect safety, including new ways to protect their online privacy and identity;
- ✓ How to report a range of concerns.

By the **end of secondary school**, 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 safe use of social media and the internet will also be covered in other subjects where relevant.

The school will use assemblies to raise learners' awareness of the dangers that can be encountered online. This will also be addressed through national agendas such as Safer Internet Day.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home. This policy will also be shared with parents on our website.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Principal 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.

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that learners understand what it is and what to do if they become aware of it happening to them or others. We will ensure that learners 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 learners, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers/form teachers will discuss cyber-bullying with their class/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 personal, social, health and economic (PSHE) education, and other subjects where appropriate.

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 learners, 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 learners' 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 learners will be carried out in line with the school's Behaviour Policy.

7. Acceptable Use Policy (AUP)

All staff, volunteers and governors are expected to read and agree the Acceptable Use Policy, Appendix 1. Visitors will be expected to read and agree to the school's terms on acceptable use if appropriate.

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 learners, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

8. Learners using mobile devices in school

8.1 Learners in the primary and secondary phase

Learners in the secondary phase may bring mobile devices into school, but are not permitted to use them during the school day. All phones are turned off before entering the school grounds and they are not to be used until they have left site.

Any breach of the acceptable use agreement by a learner may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

8.2 Learners in the VI form

Learners in VI form can bring devices on site and use these in the designated VI Form area for the purpose of research and study, but not outside this area, e.g. in corridors etc. This is to ensure we do not compromise the ethos and rules of the rest of the school. Phones should be switched off when moving around the building and attending lessons.

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, as set out in 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 the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the ICT Lead.

Work devices must be used solely for work activities.

10. How the school will respond to issues of misuse

Where a learner misuses the school's ICT systems or internet, we will follow the procedures set out in our 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/staff code of conduct. 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.

11. Training

All new staff members will carry out e-safety training as part of their safeguarding induction. All teachers and support staff working directly in the classroom will carry out more in-depth training provided by Northamptonshire Safeguarding Children Partnership. This e safety course will cover safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL/Deputy DSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years.

Volunteers will receive appropriate training and updates, where applicable.

12. Monitoring arrangements

The DSL logs all safeguarding issues related to online safety. This information is held on My Concern.

This policy will be reviewed every year by the Designated Safeguarding Lead. At every review, the policy will be shared with the governing body.

13. 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;
- ✓ICT and internet acceptable use policy.

Appendix 1 *(Taken from Wootton Park Online Safety Policy)*

Wootton Park School
ICT Acceptable Use Policy Agreement (AUP) for Learners & Parents / Carers

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

Acceptable Use Policy Agreement
I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

This Acceptable Use Policy Agreement is intended to ensure:

- learners will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to ensure that learners will have good access to digital technologies to enhance their learning and will, in return, expect the learners to agree to be responsible users.

For my own personal safety:

- I understand that the 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 not arrange to meet people off-line that I have communicated with on-line without parental knowledge.
- 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 the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school systems or devices for on-line gaming, on-line gambling, internet shopping, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.

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.
- If working remotely I will adhere to the same rules outlined in this policy.

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

- I will only use my own personal devices (mobile phones / USB devices etc) in school if I have permission). I understand that, if I do use my own devices in the school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- 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, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- 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 only use social media sites with permission and at the times that are allowed.

When using the internet for research or recreation, 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 try to 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 the 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 and where they involve my membership of the school community (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 will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, exclusions, contact with parents and in the event of illegal activities involvement of the police.

I have read and understand the above and agree to follow these guidelines when: • I use the school systems and devices (both in and out of school) • I use my own devices in the school (when allowed) eg mobile phones, gaming devices USB devices, cameras etc. • I use my own equipment out of the school in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school email etc.	
Signed (Learner):	**Date:**
Signed (Parent):	**Date:**

Wootton Park School
ICT Acceptable Use Policy Agreement (AUP) for staff, governors, volunteers and visitors

Acceptable Use Policy Agreement
I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for *learners*, and will, in return, expect staff and volunteers to agree to be responsible users.

For my professional and personal safety:

- I understand that the Wootton Park School will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, 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 immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using Wootton Park systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission. I will not use my personal equipment to record these images, unless I have permission to do so.
- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with learners and parents/carers using official school systems. Any such communication will be professional in tone and manner. (I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the *school/academy*:

- When I use my mobile devices in school, I will follow the rules set out in this agreement, in the same way as if I was using Wootton Park equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the Wootton Park ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School's Data Policy.
- I understand that data protection policy requires that any staff or learner data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

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

- I understand that this acceptable use policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this acceptable use agreement that action may be taking in line with the school's Disciplinary Policy. In the event of illegal activities, the police will be notified.

I have read and understand the above and agree to use the school digital technology systems, both in and out of school, and my own devices (in school and when carrying out communications related to the school) within these guidelines.	
Signed (Staff/Volunteer)	**Date:**