E-Safety Policy

Written by E.Besharati

July 2020

Approved by Governors.

30.9.20

Review date: July 2021

Rationale
New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning.
Children and young people should have an entitlement to safe internet access at all times. 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
- Unauthorized 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
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

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

Monitoring the impact of the policy
The school will monitor the impact of the policy using:
- Logs of reported incidents on CPOMs which is monitored regularly by executive headteachers/base leaders.
- Internal monitoring data for network activity is done through Schools IT.
- Smoothwall user logs. Our technician can access these logs to see which users accessed which web sites at which times; we can also contact schools IT to give us this data.
- We also have a heightened filtering service applied to google safe search, 'De-Crypt' and Prevent

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 at least annually 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 (Robert Stockdale) 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 executive head teacher in regards to training, identified risks and any incidents.
    - Report to governors on online safety issues that arise

Head teacher and Base Leaders
Reporting to the governing body, the executive head teachers have overall responsibility for online safety within our school. The day to day management of this will be delegated to the base leaders. 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 and governing body, parents.
- The Headteacher and Base 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 Leader.

E-Safeguarding Leader

The E-Safety Leader for the Federation is Ella Besharati. Base Leaders are responsible for day to day management of online safety in schools.

The E-Safeguarding Leader:

- Takes day to day responsibility for e-safeguarding issues and has a leading role in establishing and reviewing the school e-safeguarding policy.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an Esafeguarding incident taking place.
- Receives reports of E-safeguarding incidents and creates a log of incidents to inform future E-safeguarding developments via the IT technician.

IT Technician
The school IT technician is James Fowler. He ensures:
- That the school's ICT infrastructure is secure and is not open to misuse or malicious attack.
- That he keeps up to date with E-safeguarding technical information and updates the E Safety leader or computing coordinator as relevant.
- That monitoring software and anti-virus software is implemented and updated.

Teaching and Support Staff
Teaching and support staff are responsible for ensuring that:
- They have an up to date awareness of E-safeguarding matters and of the current school E-safeguarding policy.
- They have read, understood the school Staff Acceptable Use Policy / Agreement (AUP)/Social Networking/Mobile phones in School Policy.
- They report any suspected misuse or problem to the E-safeguarding leader for investigation.
- Digital communications with pupils (email) should be on a professional level and only carried out using official school systems.
- E-safeguarding issues are embedded in all aspects of the curriculum and other school activities. E - Safety lessons are taught through the computing scheme of work. Internet safety day is marked annually with raised awareness.
- Pupils understand and follow the school E-safeguarding and acceptable use policy.
- They are aware of E-safeguarding issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices

Designated Lead for child protection
The Headteachers and Base leaders are the Designated Leaders for Child Protection. They understand E-safeguarding issues which would trigger the Safeguarding policy and are 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 Children
- Are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign to continue to be given access to school systems.
- Children are aware that breaking the AUP would cause them to follow sanctions laid out in the Behaviour Policy.

Parents / Carers
The school will take every opportunity to help carers / parents to understand issues related to E-Safety. We will assist parents to understand key issues in the following ways:
- Parents' E-safety evening presentation.
- Regular newsletters offer parents advice on the use of the internet and social media at home.
- Information on the school website
- Parents are asked to discuss the pupil 'Acceptable Use Policy' with their children.
- Parents are asked to read their own Parents' Acceptable Use Policy.

Volunteer Users
Volunteer users/ visitors and volunteers will inform the Headteacher or Base Leaders of any web sites they wish to access. No person can log on to the internet without a user account or the Internet password. A community user account with minimal privileges will be given after discussion of the sites they wish to access. Community users are asked to sign the Volunteers Users Acceptable Use Policy.

Education – Pupils

The education of pupils in E-safeguarding is an essential part of the school's E-safeguarding provision. Children and young people need the help and support of the school to recognise and avoid E-safeguarding risks and build their resilience. 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. 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. The boundaries of use of the ICT equipment and services in this school are given in the pupil acceptable use policy; any deviation or misuse of ICT equipment or services will be dealt with in accordance to the behaviour policy.

Education - Staff Training

It is essential that all staff receive E-safeguarding training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A Staff meeting covering E-safety will take place annually. This will be delivered by a member of Ella Besharati following CEOP training
- An audit of the E-safeguarding training needs of all staff will be carried out regularly.
- All new staff should receive E-safeguarding training as part of their induction programme, ensuring that they fully understand the school E-safeguarding policy and Acceptable Use Policies.

Education - Governor

Training Governors should take part in E-safeguarding training / awareness sessions. E-Safety training is offered annually for governors. This may be delivered by North Yorkshire consultants or by PCOS Esafety officers Internet Provision The school Internet is provided by Schools IT, North Yorkshire County Network, a DFE accredited educational internet service provider. All sites are filtered using the Smoothwall filtering system which also generates reports on user activity.

Use of digital and video images - Photographic, Video, Phones (See Mobile phone Use in School Policy)

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images online.

- Staff are allowed to take digital / video images to support educational aims. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Photographs of children published on the website should not contain names.
- Pupils' full names will not be used anywhere on a website or blog.
- Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website, social media, newspaper or press. Personal Data Protection Staff must ensure that they:
- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are set to 'sleep mode' at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices such as memory sticks. Passwords All users (adults and children) will have responsibility 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
- Passwords for new users, and replacement passwords for existing users can be allocated by James Fowler, IT technician.
- Users will change their passwords regularly.

Prevent – Anti Radicalisation and extremism

School is aware that vulnerable children and adults may be exposed to terrorist propaganda through social media and the internet. The school is committed to ensuring all children are safeguarded and through the implementation of the child protection policy it ensures that this incorporates E-Safety.

Pupil Acceptable Use Policy Agreement
Reception, Year 1 and Year 2

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. Children have an entitlement to safe access when using the internet.

To stay SAFE online and on my devices:

1. I only USE devices or apps, sites or games if a trusted adult says so
2. I ASK for help if I'm stuck or not sure
3. I TELL a trusted adult if I'm upset, worried, scared or confused
4. If I get a FUNNY FEELING in my tummy, I talk to an adult
5. I look out for my FRIENDS and tell someone if they need help
6. I KNOW people online aren't always who they say they are
7. Anything I do online can be shared and might stay online FOREVER
8. I don't keep SECRETS or do DARES AND CHALLENGES just because someone tells me I have to
9. I don't change CLOTHES in front of a camera
10. I always check before SHARING personal information
11. I am KIND and polite to everyone

Class signed:

KS2 (Y3-6) Pupil Acceptable Use Policy Agreement

This agreement will help keep me safe and help me to be fair to others

1. I learn online – I use the school's internet and devices for schoolwork, homework and other activities to learn and have fun. School internet and devices are monitored.
2. I ask permission – Whether at home or school, I only use the devices, apps, sites and games I am allowed to, at the times I am allowed to.
3. I am creative online – I don't just spend time on apps, sites and games looking at things from other people. I get creative to learn and make things.
4. I am a friend online – I won't share anything that I know another person wouldn't want shared, or which might upset them. And if I know a friend is worried or needs help, I will remind them to talk to an adult, or even do it for them.
5. I am a secure online learner – I keep my passwords to myself and reset them if anyone finds them out. Friends don't share passwords!
6. I am careful what I click on – I don't click on unexpected links or popups, and only download or install things when I know it is safe or has been agreed by trusted adults. Sometimes add-ons can cost money, so it is important I always check for these too.
7. I ask for help if I am scared or worried – I will talk to a trusted adult if anything upsets me or worries me on an app, site or game – it often helps. If I get a funny feeling, I talk about it.
8. I know it's not my fault if I see or someone sends me something bad – I won't get in trouble, but I mustn't share it. Instead, I will tell a trusted adult. If I make a mistake, I don't try to hide it but ask for help.
9. I communicate and collaborate online – with people I already know and have met in real life or that a trusted adult knows about.
10. I know new online friends might not be who they say they are – I am careful when someone wants to be my friend. Unless I have met them face to face, I can't be sure who they are.
11. I check with an adult before I meet an online friend face to face for the first time, and I never go alone.

12. I don't do live videos (livestreams) on my own – and always check if it is allowed. I check with a trusted adult before I video chat with anybody for the first time.

13. I keep my body to myself online – I never get changed or show what's under my clothes in front of a camera. I remember my body is mine and no-one should tell me what to do with it; I don't send any photos or videos without checking with a trusted adult.

14. I say no online if I need to – I don't have to do something just because a friend dares or challenges me to do it, or to keep a secret. If I get asked anything that makes me worried, upset or just confused, I should say no, stop chatting and tell a trusted adult immediately.

15. I tell my parents/carers what I do online – they might not know the app, site or game, but they can still help me when things go wrong, and they want to know what I'm doing.

16. I am private online – I only give out private information if a trusted adult says it's okay. This might be my address, phone number, location or anything else that could identify me or my family and friends; if I turn on my location, I will remember to turn it off again.

17. I am careful what I share and protect my online reputation – I know anything I do can be shared and might stay online forever (even on Snapchat or if I delete it).

18. I am a rule-follower online – I know that apps, sites and games have rules on how to behave, and some have age restrictions. I follow the rules, block bullies and report bad behaviour.

19. I am not a bully – I do not post, make or share unkind, hurtful or rude messages/comments and if I see it happening, I will tell my trusted adults.

20. I am part of a community – I do not make fun of anyone or exclude them because they are different to me. If I see anyone doing this, I tell a trusted adult.

21. I respect people's work – I only edit or delete my own digital work and only use words, pictures or videos from other people if I have their permission or if it is copyright free or has a Creative Commons licence.

22.I am a researcher online – I use safe search tools approved by my trusted adults. I know I can't believe everything I see online, know which sites to trust, and know how to double check information I find.

I have read and understood this agreement. If I have any questions, I will speak to a trusted adult
at school that includes your teachers, teaching assistants and lunchtime supervisors, breakfast or after school club staff.

Class Signed: ----------Dat ----------

Staff, Governor (and Volunteer) Acceptable Use Policy Agreement

Aims

New technologies have become integral to the lives of children and young people in today's society, both within school and in their lives outside school. The internet and other digital information and communications 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. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times. This AUP works alongside our Esafety and GDPR statement on intent.

What is an AUP?

We ask all children, young people and adults involved in the life of Upper Wharfedale Primary Federation to sign an Acceptable Use Policy (AUP), which is a document that outlines how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

Why do we need an AUP?

These rules have been written to help keep everyone safe and happy when they are online or using technology. Sometimes things go wrong and people can get upset, but these rules should help us avoid it when possible, and be fair to everybody. School systems and users are protected and monitored by security and filtering services to provide safe access to digital technologies. This means anything on a school device or using school networks/platforms/internet may be viewed by one of the staff members who are here to keep your children safe. We tell your children that they should not behave any differently when they are out of school or using their own device or home network. What we tell pupils about behaviour and respect applies to all members of the school community.

If you have any questions about this AUP or our approach to online safety, please speak to Mrs Besharati (E-Safety Leader) or your child's class teacher.

All staff, governors and volunteers should read the UWPF E-Safety Policy which also links to other important policies (e.g. Safeguarding Policy, Behaviour Policy,).

You agree to:

1. I have read and understood UWPF's full ESafety Policy and agree to uphold the approaches outlined there, both for my behaviour as an adult and enforcing the rules for pupils/students. I will report any breaches or suspicions (by adults or children) in line with the policy without delay.

2. I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour which I believe may be inappropriate or concerning in any way to the Designated Safeguarding Lead (if by a child) or Headteacher (if by an adult).

3. I understand the responsibilities listed for my role in the school's Safeguarding Policies and agree to abide by these.

4. I understand that school systems and users are protected by security, monitoring and filtering services, and that my use of school devices (regardless of time, location or internet connection) and networks/platforms/internet/other technologies, including encrypted content, is monitored/captured/viewed by these systems and/or relevant/authorised staff members.

5. I understand that I am a role model and will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology, including social media, e.g. by:

- Not sharing other's images or details without permission.
- Refraining from posting negative, threatening or violent comments about others, regardless of whether they are members of the school community or not.

6. I will not contact or attempt to contact any pupil or to access their contact details (including their usernames/handles on different platforms) in any way other than school-approved and school-monitored ways, which are detailed in the school's Esafety Policy. will report any breach of this by others or attempts by pupils to do the same to the headteacher.

7. Details on social media behaviour, the general capture of digital images/video and on my use of personal devices is stated in the full Esafety policy. If I am not sure if I am allowed to do something in or related to school, I will not do it.

8. I understand the importance of upholding my online reputation, my professional reputation and that of the school), and I will do nothing to impair either. More guidance on this point can be found in this Online Reputation guidance for schools.

9. I agree to adhere to all provisions of the school Data Protection Policy Data Protection Policy at all times, whether or not I am on site or using a school device, platform or network, and will ensure I do not access, attempt to access, store or share any data which I do not have express permission for. I will protect my passwords/logins and other access, never share credentials and immediately change passwords and notify the Headteacher if I suspect a breach. I will not store school-related data on personal devices, storage or cloud platforms. USB keys, where allowed, will be encrypted, and I will only use safe and appropriately licensed software, respecting licensing, intellectual property and copyright rules at all times.
Note: Governors will receive information via password-protected NYCC email that is necessary to perform their roles. They should ensure the never share their email passwords with anyone. Their devices should be password protected and notify the Headteacher if they suspect a breach.

10. I will use school devices and networks/internet/platforms/other technologies for school business and I will never use these to access material that is illegal or in any way inappropriate for an education setting. I will not attempt to bypass security or monitoring and will look after devices loaned to me.

11. I will not support or promote extremist organisations, messages or individuals, nor give them a voice or opportunity to visit the school. I will not browse, download or send material that is considered offensive or of an extremist nature by the school.

12. I understand and support the commitments made by pupils/students, parents and fellow staff, governors and volunteers in their Acceptable Use Policies and will report any infringements in line with school procedures.

13. I will follow the guidance in the E- Safety Policy for reporting incidents – I understand the principle of 'safeguarding as a jigsaw' where my concern might complete the picture. I have read the sections on handing incidents and concerns about a child in general, sexting, upskirting, bullying, sexual violence and harassment, misuse of technology and social media.

14. I understand that breach of this AUP and/or of the school's full ESafety Policy may lead to appropriate staff disciplinary action or termination of my relationship with the school and where appropriate, referral to the relevant authorities.

Name: Position:
Signed: Date:

Parental Acceptable User Policy (AUP)

What is an AUP?

We ask all children, young people and adults involved in the life of Upper Wharfedale Primary Federation to sign an Acceptable Use Policy (AUP), which is a document that outlines how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

Why do we need an AUP?

These rules have been written to help keep everyone safe and happy when they are online or using technology. Sometimes things go wrong and people can get upset, but these rules should help us avoid it when possible, and be fair to everybody. School systems and users are protected and monitored by security and filtering services to provide safe access to digital technologies. This means anything on a school device or using school networks/platforms/internet may be viewed by one of the staff members who are here to keep your children safe. We tell your children that they should not behave any differently when they are out of school or using their own device or home network. What we tell pupils about behaviour and respect applies to all members of the school community.

If you have any questions about this AUP or our approach to online safety, please speak to Mrs Besharati (E-Safety Leader) or your child's class teacher.

1. I understand that the schools in the Upper Wharfedale Primary Federation use technology as part of the daily life of the school when it is appropriate to support teaching & learning and the smooth running of the school, and to help prepare the children and young people in our care for their future lives.

2. I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials, including behaviour policies and agreements, physical and technical monitoring, education and support and web filtering. However, the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies, which can sometimes be upsetting.

3. I understand that internet and device use in school, and use of school-owned devices, networks and cloud platforms out of school may be subject to filtering and monitoring. These should be used in the same manner as when in school.

4. I will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.

5. The impact of social media use is often felt strongly in schools, which is why we expect certain behaviours from pupils when using social media. I will support the school's social media policy and not encourage my child to join any platform where they are below the minimum age.

6. I will follow the school's digital images and video policy, which outlines when I can capture and/or share images/videos. I will not share images of other people's children on social media and understand that there may be cultural or legal reasons why this would be inappropriate or even dangerous. The school sometimes uses images/video of my child for internal purposes such as recording attainment, but it will only do so publicly if I have given my consent on the relevant form at the beginning of each school year.

7. I understand that for my child to grow up safe online, s/he will need positive input from school and home, so I will talk to my child about online safety (NB: the recent LGfL DigiSafe survey of 40,000 primary and secondary pupils found that 73% of pupils trust their parents on online safety, but only half talk about it with them more than once a year). Understanding human behaviour is more helpful than knowing how a particular app, site or game works.

8. I understand that whilst home networks are much less secure than school ones, I can apply child safety settings to my home internet. Internet Matters provides guides to help parents do this easily for all the main internet service providers in the UK.

9. I understand that it can be hard to stop using technology sometimes, and I will talk about this to my children, and refer to the principles of the Digital 5 A Day: childrenscommissioner.gov.uk/our-work/digital/5-a-day/ 10. I understand and support the commitments made by my child in the Acceptable Use Policy (AUP) which s/he has signed, and which can be seen in the e-safety policy.

I can find out more about online safety by reading the full ESafety Policy on our school website and can talk to Mrs Besharati (E-Safety Leader) or your child's class teacher if I have any concerns about my child/ren's use of technology, or about that of others in the community, or if I have questions about online safety or technology use in school.

Social Media

In line with our staff acceptable use policy we ask parents not to befriend teachers on social media unless already friends before your child attended the school or before they worked at school. For the protection of our children and the school's reputation we ask you to refrain from discussing school issues on social media, if you have anything you want to discuss please follow the usual protocol setting up meetings with class teachers, Base leaders, Headteachers or governors depending on your issue.

Use of Digital / Video Images

The use of digital / video images plays an important part in learning activities. Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons or for training support. Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media (parents tick parental permission sheet in admission pack). We will comply with the Data Protection Act and request parents / carers permission before taking images of members of the school. We will also ensure that when images are published that the young people are only identified by their first name only. To protect all children at our school we will endeavour to provide photographs or DVDs of key school events at a low cost to you. To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.

Name:

Signed: Date: