Burlington Junior School

Shaping Positive Futures

Achieving Our Full Potential

Date adopted	October 2024
Date approved by chair of Committee	October 2024
Review date	October 2025

Online Safety
Filtering and Monitoring Policy

Contact details
Email:- burlington.juniors@eastriding.gov.uk
Telephone:- 01262 674487

This policy applies to all members of the school community (including staff, learners, volunteers, parents and carers, visitors, community users) who have access to and are users of our school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

At Burlington Junior School we believe that computing is central to all aspects of learning; for adults and children in both the school and the wider community. Provision should reflect the rapid developments in technology.

Computing in the 21st Century is an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, we need to build in the use of these technologies in order to equip our young people with the skills to access lifelong learning and employment.

We believe that 'Online Safety' is the responsibility of the whole community, and everyone has their part to play in ensuring all members of the community are able to benefit from the opportunities that technology provides for teaching and learning whilst remaining safe when accessing these. Due to our whole school approach, we recognise that all members of our school and community have a responsibility in upholding and supporting safe practice in their classrooms and follow our 'Online Safety, Filtering and Monitoring' policies and procedures.

Once staff are aware of the policies and procedures in school, they will then be required to sign our Acceptable User Policy (AUP) agreement to declare understanding of our protocol before using any technology in school (Appendix 2).

This policy is implemented in accordance with our compliance with DfE statutory guidance KCSiE 2024. Online Safety, filtering and monitoring is also detailed in the school Child Protection and Safeguarding Policy 2024.

1. Aims

The importance of safeguarding children from potentially harmful and inappropriate online material is recognised and understood, along with the fact that technology is a significant component in many safeguarding and wellbeing issues.

To address this and in light of the 4 categories of risk outlined below, we will adopt a whole school approach involving a number of measures and approaches with the aim of:

- Having robust processes (including filtering and monitoring systems) in place to ensure the online safety of pupils, staff, volunteers and governors
- Protecting and educating the whole school community in safe and responsible use of technology, including mobile and smart technology
- Setting clear guidelines for the use of mobile phones for the whole school community
- Establishing clear mechanisms to identify, intervene in and escalate any incidents or concerns, where appropriate

The approach to online safety is based on addressing the following 4 categories of Risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education 2024, and its advice for schools on:

- Teaching online safety in schools
- Online Filtering and Monitoring
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and health education
- Searching, screening and confiscation

It also refers to the DfE'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 pupils' 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

KCSiE 2024, outlines the need for staff and Governors to receive training covering online safety (including Filtering and Monitoring) and that it is essential that there is a whole school approach towards online safety, including training, curriculum content and teaching, communication with parents/carers and school IT resources / devices / network (appropriate filtering and monitoring etc). The Governing Body will retain strategic oversight of this and ensure that appropriate processes and procedures are established and maintained.

The Governing Body will

- Make sure that the school has appropriate filtering and monitoring systems in place and review their effectiveness
- Review the DfE's filtering and monitoring standards, and discuss with IT staff and service providers about what needs to be done to support the school to meet these standards
- Make sure the DSL takes lead responsibility for understanding the filtering and monitoring systems in place as part of their role
- Make sure that all staff undergo safeguarding and child protection training, including online safety and that such training is regularly updated and is in line with advice from the safeguarding partners
- Make sure staff understand their expectations, roles and responsibilities around filtering and monitoring as part of safeguarding training

- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children.
- 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 (appendix 2)
- As part of their oversight role, our Governing body will ensure staff safeguarding and child protection training includes online safety which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring.

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

The DSL will respond to online safety concerns in line with Safeguarding / Child Protection and any other associated policies, including our Anti-bullying Policy and Behaviour Policy:

- Internal sanctions and/or support will be implemented as appropriate.
- Where necessary, concerns will be escalated and reported to relevant partner agencies in line with local policies and procedures.

The DSL takes lead responsibility for online safety, filtering and monitoring in school as the management of this is a safeguarding issue. The DSL roles include:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are logged on CPOMS 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 body
- If users discover a website with inappropriate content, this should be reported the DSL or DDSL.

- If users discover a website with potentially illegal content, this should be reported immediately to the DSL or DDSL. The school will report this to appropriate agencies including the filtering provider, LA, **Child Exploitation and Online Protection (CEOP)**

This list is not intended to be exhaustive.

3.4 The ICT Manager

The school uses a filtered Internet service. The filtering is provided through East Riding of Yorkshire Council, along with the Smoothwall filter.
The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept 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 monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

This list is not intended to be exhaustive.

3.5 All Staff and Volunteers

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 (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy. All online safety issues are logged using the CPOMS system and the DSL and headteacher are informed immediately.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

3.6 Parents

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 (appendices 1 and 2)

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 resource sheet – Childnet International
- Healthy relationships – Disrespect Nobody

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 terms on acceptable use (appendix 2).

4. Filtering and Monitoring

In relation to filtering and monitoring, we will adhere to DfE filtering and monitoring standards on school devices and school networks, and in so doing will:

• identify and assign roles and responsibilities to manage filtering and monitoring systems.

• review filtering and monitoring provision at least annually.

• block harmful and inappropriate content without unreasonably impacting teaching and learning.

• have effective monitoring strategies in place that meet their safeguarding needs

Burlington Junior School uses a filtered Internet service (Smoothwall) provided by East Riding of Yorkshire Council. The school will liaise closely with its service provider to ensure they are kept updated on any new and improved filtering systems and software. Burlington Junior School have established mechanisms to identify, intervene in, and escalate any concerns where appropriate.

Adherence to the standards, and the effectiveness of the filtering systems in place will be regularly reviewed each term and involve discussion with IT staff and service providers and the nominated Governor and SLT member for this area of safeguarding as well as the DSL (who will lead and retain responsibility for this). This will be supported by an annual risk assessment that considers and reflects the risks faced by our school community.

Filtering breaches or concerns identified through internal monitoring will be recorded and reported to the DSL, who will review and respond as appropriate. Staff will record the URL of the site and serial number of the device and keep the device safe for further investigation.

The local authority will send a daily, electronic, filtering report and will contact the school on the day should a breach or concern arise. The DSL and DDSL will view these daily reports and respond appropriately. These will be monitored and assessed as part of the termly monitoring schedule.

Burlington Junior School uses a wide range of devices and technology systems to facilitate internal and external communication, teaching and information storage. The school Acceptable User Policy and Online Safety Policy underpin the operation of all school owned devices and systems along with safety and security measures in place.

All communication with pupils/students and parents/carers will take place using School provided or approved communication channels; for example, School provided email accounts and phone numbers and/or agreed systems: Google Classroom, Microsoft 365 or equivalent etc. Any pre-existing relationships or situations which mean this cannot be complied with will be discussed with the DSL.

Any access to materials believed to be illegal, will be considered as a safeguarding issue and appropriate action taken to address concerns.

All staff will log behaviour and safeguarding issues related to online safety on CPOMS see (Child Protection and Safeguarding Policy). Once logged they will inform the headteacher or DSL of the safety issues.

This policy will be reviewed every year by the DSL. At every review, the policy will be shared with the governing body. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

5. Educating Pupils about Online Safety

Burlington Junior School will ensure a comprehensive whole school curriculum response is in place to enable all pupils to learn about and manage online risks effectively as part of providing a broad and balanced curriculum. PSHE and computing lessons focus in depth on these issues.

Pupils will be taught about online safety as part of the curriculum:

The text below is taken from the National Curriculum computing programmes of study.

It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

All primary schools have to teach:

- Relationships education and health education in primary schools

Pupils 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**, pupils 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
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know
- The safe use of social media and the internet will also be covered in other subjects where relevant.
- Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

6. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website, Class Dojo or Google Classroom. This policy will also be shared with parents.

Online safety, Filtering and Monitoring 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.

7. Cyber-bullying

7.1 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.

7.2 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. This will be discussed in classes or through whole school 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. Jigsaw is used across the school to teach cyber-bullying in an age-appropriate way.

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

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.

7.3 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 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, 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*

* Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element. See 'Screening, Searching and Confiscation Policy'.

Any searching of pupils will be carried out in line with:

- The DfE's July 2023 latest guidance on screening, searching and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

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

8. 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 1-2). 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, 2.

9. Using email and messaging facilities

- Staff and pupils should use approved e-mail accounts allocated to them by the school, and be aware that their use of the school e-mail system can be monitored and checked.
- Pupils are introduced to email as part of the Computer Science Scheme of Work.
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.
- Pupils will be reminded when using e-mail about the need to send polite and responsible messages, about the dangers of revealing personal information, the dangers of opening e-mail from an unknown sender, or viewing/opening attachments.
- Staff and pupils are not permitted to access personal e-mail accounts during school.
- Communication between staff and pupils or members of the wider school community should be professional and related to school matters only.
- Any inappropriate use of the school e-mail system, or the receipt of any inappropriate messages by a user, should be reported to a member of staff immediately.
- Class Dojo, Emails and text messages will be the main means of communication between staff and parents.

10. Using mobile phones

- Staff will not be expected to use personal mobile phones in any situation where their mobile phone number or other personal details may be revealed to a pupil or parent.
- Staff must not use their mobile phone in front of pupils unless in an emergency situation.
- Staff must not use their personal mobile phone to take or store photographs of pupils.
- If pupils bring mobile phones to school, they will be handed in to their class teacher at the start of the day.

11. Using new technologies

- As a school we will keep abreast of new technologies and consider both the benefits for learning and teaching and also the risks from an online safety, Filtering and Monitoring point of view.
- We will regularly amend the online safety policy to reflect any new technology that we use, or to reflect the use of new technology by pupils which may cause an online safety, Filtering and Monitoring risk.

12. Protecting personal data

- We will ensure personal data is recorded, processed, transferred and made available according to the Data Protection Act 2018.
- Staff will ensure they properly log-off from a computer terminal after accessing personal data.
- Staff will not remove personal or sensitive data from the school premises without permission from the head teacher, and without ensuring such data is kept secure.
- Staff will use encrypted data storage for all school work on and off site.

13. Publishing pupil's work and images

- On a child's entry to the school, all parents/guardians will be asked to give permission for their child's photo to be taken and to use their child's work/photos in the following ways:
- On the school web site
- In display material that may be used in the school's communal areas
- In display material that may be used in external areas, i.e. exhibition promoting the school
- General media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically.)
- Pupils' names will not be published alongside their image and vice versa without permission from the parents. Full names will not be published.

14. Remote learning

At Burlington Junior School during any partial or complete national lockdown forcing the closure of schools our remote learning will ensure that we stay connected as a school community. The curriculum provided will allow a continuation of learning and will deliver important support for pupil's well-being.
The platform that will be used for all remote learning sessions is Google Classroom, which is available through any device where Google is accessible. Information relating to any remote learning sessions including documents, video links and any other relevant material will be posted within Google Classroom. It is vital that children access Google Classroom every morning so that they can keep up to date with newly posted lessons and activities that they will be required to hand in.
In order to create a stimulating yet safe environment for our pupils, there are key areas which teachers must abide by:

- We must have consent from parents/ carers to access the remote sessions. (Appendix 3)
- Teachers must be familiar with the functions of Google Classroom including mute settings.
- Any remote sessions should be hosted and supervised by the class teacher.
- When using Google Meet, the pupils must exit first and the teacher should end the call to ensure unsupervised conversations do not occur.
- Teachers should ensure that during a Google Meet call they use an appropriate background as well as suitable clothing for both staff and pupils.

15. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Keeping operating systems up to date – always install the latest updates
- Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2.

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

16. 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 our policies on behaviour and ICT and internet 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 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.

17. Training

All new staff members will receive training, as part of their induction, on safe internet use, Filtering and Monitoring, 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).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- The importance of Filtering and Monitoring, school procedure and policy
- Children can abuse their peers (child on child) online through:
    - Abusive, harassing, and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up
- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and DDSL will undertake child protection and safeguarding training, which will include Online Safety, Filtering and Monitoring, at least every 3 years. They will also update their knowledge and skills on the subject at regular intervals, and at least annually.

Governors will receive training on Safe Internet use, Filtering and Monitoring 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.

18. Links with other policies

This online safety policy is linked to our:

- Child Protection and Safeguarding Policy
- Code of Conduct Policy
- Data protection policy and privacy notices
- Complaints Procedure
- Behaviour Policy
- Searching, Screening and Confiscation Policy
- Low Level Concern Policy

Appendix 1
Acceptable Use Policy for Pupils

You can use the computers and other devices in school to access the Internet to help you with your learning. These rules will help make sure the Internet is a safe and fun place for everyone in school. You will need to agree to follow these rules whenever you use ICT at school.

- I will ask permission from a member of staff before using the internet.
- I will only use the computers and other devices for school work and homework.
- I will not access files that belong to other people.
- I will only use equipment or files I bring from home, such as my mobile phone or files on a USB stick, if the school lets me, and for activities the school agrees to.
- I will only send messages to people I know, or my teacher has approved, as part of my lesson.
- The messages I send, and the work I do, will be polite and responsible, and will not contain anything that might upset someone else.
- I will only open attachments in messages I receive, or download a file, if I trust the person who sent it or the website it is from, and I've checked with my teacher that it is safe.
- I will keep my username and password safe by not telling anyone else.
- I will not change any settings on the computers and other devices I use at school.
- I will not install or delete any software on the computers and other devices I use

at school.

- I will not give away any of my personal information, or the personal information of people I know, over the Internet. This includes my full name, address, phone numbers, photographs and videos of me and my friends, or the name of my school unless my teacher has checked it is safe.
- If something happens whilst using a computer or school device, and I am not sure what I should do next, I will ask a member of staff to help me.
- To help protect other pupils and myself, I will tell a teacher if I see anything I am unhappy with or I receive messages I do not like.
- I understand that the school may check my computer files, the Internet sites I visit, the messages I send and anything else I do to make sure I am keeping myself and others safe.
- I understand that if I do not follow these rules and other guidance from the school as best as I can then I may not be allowed to use the Internet or any of the school's ICT equipment.

Appendix 2 Acceptable Use Policy for Staff and other adults in school

These statements are designed to ensure staff and other adults in school are aware of their professional responsibilities when using the ICT systems provided. All staff should follow the guidelines at all times. You are responsible for your behaviour and actions when accessing the Internet at school, whether on your own or school equipment, and when using school ICT equipment at other locations such as your home. Any use of school ICT systems will be for professional purposes.

- Usernames, passwords and other logon details should be kept secure and not revealed to anyone else. Care should be taken to ensure you logout when not actively using the ICT systems. You should not allow an unauthorised person to access the school ICT systems, e.g. by logging in for them.
- Any online activity should not harass, harm, offend or insult other users.
- You will not search for, download, upload or forward any content that is illegal, or that could be considered offensive by another user. If you accidentally encounter such material you should follow your school's procedure and report this immediately.
- You should not download or install any hardware or software without permission. If you have responsibility for installing software you should be confident it is adequately licensed and appropriate for educational use.
- Ensure that any files on removable media (e.g. USB drives, CDs) are free from viruses and other malware before use and that such devices are not used for carrying sensitive data or details of pupils, parents or other users without suitable security and without permission from the Headteacher.
- Any electronic communications should be related to schoolwork only, and should be through school e-mail addresses or other school systems. It is not acceptable to contact pupils using personal equipment or personal contact details, including your own mobile phone or through your personal social network profiles.
- Any online activity, including messages sent and posts made on websites, and including activity outside of school, should not bring your professional role or the name of the school into disrepute.
- Any still or video images of pupils and staff should be for professional purposes only. They should be taken on school equipment, and stored and used onsite.

Such images should not be taken off-site without permission and valid reason.

- You will not give out your personal details, or the personal details of other users, to pupils or parents or on the Internet. In particular you should ensure your home address, personal telephone numbers and email accounts are not shared with children, young people or parents.
- You should ensure that any personal or sensitive information you use or access (e.g. SIMS data, assessment data) is kept secure and used appropriately.
- Personal or sensitive information should only be taken off-site if agreed with the Headteacher, and steps should be taken to ensure such data is secure.
- You should respect intellectual property and ownership of online resources you use in your professional context, and acknowledge such sources if used.
- You should support and promote the school Online Safety Policy, and promote and model safe and responsible behaviour in pupils when using ICT to support learning and teaching

You understand that your files, communications and Internet activity may be monitored and checked at all times to protect your own and others' safety, and action may be taken if deemed necessary to safeguard yourself or others. If you do not follow all statements in this AUP and in other school policies, you may be subject to disciplinary action in line with the school's established disciplinary procedure.

Appendix 3

Use of Google Classroom/Google Meet

Please read the following expectations in regards to your child's attitude and behaviour for home learning. This MUST be completed and signed by a parent or carer before they can join any live sessions/activities with a member of teaching staff.

1. Pupils will never use email or other communication tools to offend, intimidate, exclude or in any way 'bully' others.
2. When working collaboratively, pupils must ensure they do not interfere with, delete or alter others' work unless they are offering constructive feedback. This includes deliberately deleting, amending or editing others' saved work without their, or their teacher's, explicit permission.
3. Pupils must not change any setting on their chrome book without permission from their class teacher or other designated member of staff.
4. Pupils must report any problem, concern or incidents which they feel uncomfortable about, to their class teacher or other member of staff and refrain from sharing personal information about themselves whilst online, as detailed in the school's e-safety input.
5. Pupils must ensure they only ever use appropriate images, videos, text and other media in all their work and use of this technology.
6. Pupils must ensure that the camera on the device is not used to record anybody without their permission.
7. When using 'Google Meet' you must be dressed appropriately and join all meetings on mute.
8. When pupils are completing their lessons they must ensure they are in a room where they can concentrate without distractions.
9. When pupils are using 'Google Meet' they must be aware of any background noise that will come through their microphone when speaking.

We want every child at school to enjoy and have a positive experience using the latest technologies to enhance their remote learning. Following the above rules and guidance will help us to achieve these goals.

Pupil name:
Signed (parent): Signed (child)