WEXHAM COURT PRIMARY SCHOOL

E-Safety Policy

2024 - 2025

Date Approved:	**Spring 2024**
Date for Review:	**Spring 2025**
Approved By:	**Headteacher**

WEXHAM COURT PRIMARY SCHOOL

E-SAFETY POLICY

Preparing every child to become a successful individual in an ever evolving world.

Build belonging **Strive for excellence** **Do the right thing**

EQUALITY STATEMENT

At Wexham Court Primary School we are proud of the diversity of our students and staff and are committed to promoting a positive and inclusive culture in which all are valued and supported to fulfil their potential irrespective of their age, disability, race, religion, beliefs, sex or sexual orientation. We acknowledge that we are all influenced by implicit bias, or the stereotypes that unconsciously affect our decisions and that this can negatively impact traditionally marginalised and disenfranchised students. In all areas of our school, we strive to understand and appreciate all aspects of diversity, equality and inclusion and proactively adapt our school policies and procedures accordingly.

1. AIMS

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

Our vision acknowledges an ever-evolving world, therefore at Wexham Court we embrace technologies whilst remaining vigilant about the associated risks. Our values underpin our approach:

- *Build Belonging* – we are able to connect to a community beyond our school and network with people that we know and trust

- *Do The Right Thing* – pupils are taught to reflect on their choices and make a decision that is right for all. Pupils are to apply their knowledge of internet safety to ensuring they make positive choices for all whilst online

- *Strive For Excellence* – to embrace new technology and grow alongside it, equip pupils with the skills and knowledge they need to adapt and live successfully in the future.

The 4 key categories of risk

Our approach to online safety is based on addressing the following 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's) 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
- 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 Headteacher

The Headteacher has overall responsibility for monitoring this policy and holding staff to account for its implementation.

The Headteacher will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The Headteacher will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The Headteacher will delegate to the DSL who will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the Designated Safeguarding Lead (DSL).

The Headteacher and DSL must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The Headteacher and DSL will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs;
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

Information will be shared with the safeguarding governor and discussed during the Full Governing Body meetings.

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

3.2 The Designated Safeguarding Lead

Details of the school's Designated Safeguarding Lead (DSL) and deputies are set out in our Safeguarding and Child Protection policy, as well as relevant job descriptions.

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

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the headteacher and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly.
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks.
- Working with the IT contractor to make sure the appropriate systems and processes are in place.
- Working with the headteacher, IT contractor 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's child protection policy.
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy.

- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy.
- Updating and delivering staff training on online safety.
- Liaising with other agencies and/or external services if necessary.
- Providing regular reports on online safety in school to the headteacher and/or governing board.
- Undertaking annual risk assessments that consider and reflect the risks children face.
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively.

This list is not intended to be exhaustive.

3.3 The Governing Board

All governors will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's IT systems and the internet (appendix 3)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures

3.4 The IT Contractor

The Headteacher and DSL in conjunction with Tri-Computers will be responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually 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 IT 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 IT systems
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

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 IT systems and the internet (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1).
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and reporting to the Headteacher or DSL any incidents without delay.
- Following the correct procedures by speaking directly to the Headteacher or DSL if they need to bypass the filtering and monitoring systems for educational purposes.
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.
- 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'.
- Mobile technology assigned to a member of staff as part of their role and responsibility must have a passcode or device lock so unauthorised people cannot access the content.
- Where staff are issued mobile technology as part of their role and responsibility must ensure they lock away the correct items (e.g. iPads) each day. Staff are responsible for keeping their assigned items safe and in their care as per the IT Acceptable Use Agreement. Loss of items will incur a fine, and the staff member (not the Administrative team) is responsible for finding the lost items within 2 working days.
- No personal devices belonging to staff are to be used during lessons at school. If staff bring in their own devices, these items are not the school's responsibility nor will the school accept any responsibility for loss or damage.

This list is not intended to be exhaustive.

3.6 Parents/Carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy.
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's IT systems and internet (appendices 1 and 2).

Parents/carers 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

3.7 Visitors And Members Of The Community

Visitors and members of the community who use the school's IT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

4. EDUCATING PUPILS ABOUT ONLINE SAFETY

Pupils will be taught about online safety as part of the curriculum. All schools have to teach: Relationships education and health education in primary schools.

In Key Stage (KS) 1, pupils 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.

Pupils in Key Stage (KS) 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.
- How to report any issues outside of school and who to report to inside school.

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.

5. EDUCATING PARENTS/CARERS ABOUT ONLINE SAFETY

The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website or through parent events. This policy will also be shared with parents/carers.

Online safety will also be covered during parents' evenings.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use.
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online.

If parents/carers 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.

6. CYBER-BULLYING

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school's behaviour and anti-bullying policies.)

6.2 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. Class teachers will discuss cyber-bullying with their classes.

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.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also provides information on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected through the school website and parent events.

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 school is aware that radicalisation can happen online, any incidents will be addressed by the DSL in line with our Safeguarding and Child Protection Policy.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining Electronic Devices

The headteacher, and any member of staff authorised to do so by the headteacher (as set out in the school's behaviour policy), can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher / DSL / SLT member should the prior two not be available.
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it.
- Seek the pupil's co-operation.

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence.

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL / headteacher to decide on a suitable response. If there are images, data or files on the device that staff

reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves.

If a staff member suspects a device may contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- Not view the image.
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

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

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

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

6.4 Artificial Intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

Wexham Court Primary recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.

Children are currently taught about the dangers of AI such as deepfake pictures and information; how using AI to help complete homework or other tasks is a form of cheating. The focus of teaching around AI will be adapted according to the changes in technology and any changes that are made to Keeping Children Safe in Education.

The School will treat any use of AI to bully pupils in line with our anti-bullying and behaviour policies.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school.

Staff need to remember that any personal data or data that would make the school/ child or teacher recognisable, may not be used through AI. AI currently is not protected data and can be used by companies as required.

7. ACCEPTABLE USE OF THE INTERNET IN SCHOOL

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's IT systems and the internet (appendices 1 and 2). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

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

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in appendices 1 and 2.

8. PUPILS USING MOBILE DEVICES IN SCHOOL

Pupils in Year 4 upwards may bring mobile devices into school where they walk to or from school by themselves. All devices must be handed in to the office at the start of the school day and collected at the end of the day. These items are not the school's responsibility, nor will the school accept any responsibility for any loss or damage.

9. 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.
- Not sharing the device among family or friends.
- Installing anti-virus and anti-spyware software.
- Keeping operating systems up to date by always installing the latest updates (missing full stops).
- Store their device in a safe place and not in their cars overnight.

Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in appendix 2.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the DSL or Headteacher.

10. HOW THE SCHOOL WILL RESPOND TO ISSUES OF MISUSE

Where a pupil misuses the school's IT systems or internet, we will follow the procedures set out in our policies on behaviour, IT acceptable use, Safeguarding and Child Protection and Data Protection policies. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's IT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures and 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 that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. TRAINING

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

All staff members will receive training at least once each academic year as part of the safeguarding training timetable, 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.
- Children can abuse their peers 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 do not 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 up the risks.
- 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 deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

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

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. MONITORING ARRANGEMENTS

The DSL logs behaviour and safeguarding issues related to online safety. These are reviewed half termly to see what incidents have taken place. The DSL will share trends and patterns with the SLT.

This policy will be reviewed every year by the DSL and Computing Lead, the policy will then be shared with staff and the governing board. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online and any changes made in Keeping Children Safe in Education. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. LINKS WITH OTHER POLICIES

This online safety policy is linked to our:

- Safeguarding and Child Protection policy
- Behaviour policy
- Anti-Bullying policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- IT and internet acceptable use policy
- Staff Code of Conduct

This is a true version signed by

Miss N Mehat Headteacher

Signed: Date:

Review date: Spring 2025

APPENDIX 1 – PUPIL ACCEPTABLE USE POLICY

The school has provided computers and tablets with internet access to help your learning. You have also been provided with a Microsoft Teams account. These rules will keep us safe and help us to be fair to others.

- I will only use school IT equipment for learning purposes.
- I will ask permission from a member of staff before using the internet and will only go online when an adult is in the room.
- I will only use my own login and password and never share these with others.
- I will only use Teams, whether at school or at home, to support my learning.
- I will only message my teachers on Teams, or other staff who work at the school, during school hours to support my learning.
- I will not use Teams in or out of school to message my friends or speak to other adults who do not work at the school.
- I will inform my teacher immediately if my friends or an adult who does not work at the school tries to speak to me on Teams.
- I will only open, edit and delete my own files.
- I will not download or delete any apps on the computers, laptops or iPads unless I have been given permission to do so by an adult.
- I will ensure I use the technologies carefully, never removing the iPads from the case or run with one.
- The messages I send will be polite and sensible.
- I will never give out my own or other people's name, address or phone number online.
- I will never upload any images of school activities to any social networking site.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty.
- If I see anything I am unhappy with on the computers, I will turn the screen off and tell my teacher or an appropriate adult straight away.
- I understand that the school can check my computer use and that my parents/carers can be contacted if school staff are concerned about my E-Safety.

Pupil Signed: Date:

Class:

APPENDIX 2 – IT ACCEPTABLE USE POLICY FOR STAFF, GOVERNORS AND VISITORS

These rules are designed to protect staff and visitors from E-Safety incidents and promote a safe e-learning environment for pupils. The following is considered unacceptable use of the school's IT facilities. Any breach of this policy may result in disciplinary proceedings.

Unacceptable use of the school's IT facilities includes:

- Using the school's IT facilities to breach intellectual property rights or copyright.
- Using the school's IT facilities to bully or harass someone else, or to promote unlawful discrimination.
- Breaching the school's policies or procedures.
- Any illegal conduct, or statements which are deemed to be advocating illegal activity.
- Online gambling, inappropriate advertising, phishing and/or financial scams.
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful.
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams.
- Activity which defames or disparages the school, or risks bringing the school into disrepute.
- Sharing confidential information about the school, its pupils, or other members of the school community.
- Connecting any device to the school's IT network without approval from authorised personnel.
- Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any programme, tool or item of software designed to interfere with the functioning of the school's IT facilities, accounts or data.
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel.
- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the school's IT facilities.
- Causing intentional damage to the school's IT facilities.
- Removing, deleting or disposing of the school's IT equipment, systems, programmes or information without permission from authorised personnel.
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not permitted by authorised personnel to have access, or without authorisation.
- Using inappropriate or offensive language.
- Promoting a private business, unless that business is directly related to the school.

- Using websites or mechanisms to bypass the school's filtering or monitoring mechanisms.
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way.

In addition, staff will:

- Use the school's internet, email, computers, laptops and other mobile technologies for professional purposes.
- Where staff are issued mobile technology as part of their role and responsibility must ensure they lock away the correct items (e.g. iPads) each day. Staff are responsible for keeping their assigned items safe and in their care as per the IT Acceptable Use Agreement. Loss of items will incur a fine, and the staff member (not the Administrative team) is responsible for finding the lost items within 2 working days. The fine will be £75-£100 per item.
- Password protect all school devices or systems and will not use the autosave password feature.
- Will not disclose passwords to anybody else, or use search engines to save any to file. All passwords will be stored securely. Where asked to reset passwords, staff will ensure that the password is suitably secure and not easily guessed by others.
- Any online communications with staff, parents and pupils are compatible with professional roles. Staff will ensure that they are aware of e-safety issues related to the use of social media, mobile phones, cameras and hand-held devices and that they abide by current school policies on e-safety and the staff code of conduct.
- I will ensure that digital communications with pupils (email/virtual learning environment (VLE)/voice) are on a professional level and only carried out using official school systems.
- Understand that members of staff who are found to be producing covert recordings, whether audio or visual, on any form of electronic device; whether owned by the school, or a personal device, will face disciplinary action.
- Follow the training on cyber security and filtering and monitoring, and report anything of danger.

This is not an exhaustive list. The school reserves the right to amend this list at any time. The headteacher and DSL will use their professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's IT facilities.

I confirm that I have read and understood the above and that Staff who engage in any of the unacceptable activities listed above may face disciplinary action in line with the school's policies disciplinary and staff conduct procedures.

Signed:…….

Print Name: …….

Date: ……