PAPILLON HOUSE SCHOOL

Online Safety Policy

November 2023

v.3

Contents

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff and volunteers
- Identify and support groups of pupils that are potentially at greater risk of harm online than others and understanding that all our pupils are at greater risk of harm because they are autistic.
- 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

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, anti-Semitism, 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 scam

2. Legislation and guidance

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

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

It also refers to the 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.

3. Roles and responsibilities

3.1 The Management Team

The Management Team has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The Management Team 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 Management Team 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 management team will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the Designated Safeguarding Lead (DSL).

The Management Team should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The Management Team 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 Team 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, or where there is a need to do so;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.
- Carry out termly checks on the filtering and monitoring system. These will be recorded on the online safety incident log.

All members of the management team will:

- Ensure that they have read and understood this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, takes account of the SEND needs of our pupils who all have a diagnosis of ASD and is adapted for vulnerable children and victims of abuse 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

3.2 The Director

The Director 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 (DSL)

Details of the school's designated safeguarding lead DSL and deputies are set out in our Child Protection and Safeguarding Policy as well as relevant job descriptions.

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

- Supporting the Business Manager and Director in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Business Manager and Director to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead with the Business Manager on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the Business manager and IT support to make sure the appropriate systems and processes are in place
- Working with the Business Manager, IT support 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 and record them in line with the school child protection policy (see clause 12)
- Ensuring that any online safety incidents, particularly those that arise through the School's monitoring system or that relate to staff are logged (see appendix 4) and dealt with appropriately in line with this policy (see clause 12)
- 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 (appendix 3 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Management Team
- 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.

3.4 The Business Manager

The Business Manager is 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
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents that arise through the School's monitoring system or that relate to staff are logged (see appendix 4 and clause 12) 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.

3.4 The IT Service Provider

- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Ensuring that the Schools IT consultants conduct regular security checks and monitoring of the school's ICT systems including windows updates, antivirus, backups and that any alerts for failures are acted upon.
- Maintaining the filtering and monitoring system.
- Providing filtering and monitoring reports
- Supporting follow up and following up where appropriate on any concerns arising through the system

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 2), and ensuring that pupils follow the school's terms on acceptable use (appendices 1)

- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by reporting these to the DSL
- Knowing to report to the DSL, safeguarding and technical concerns, such as:
    - Witnessing or suspecting unsuitable material has been accessed
    - Accessing unsuitable material
    - If teaching topics that may create unusual activity on the filtering logs
    - Perceiving unreasonable restrictions that affect teaching and learning or administrative tasks
    - Noticing abbreviations or misspellings that allow access to restricted material
- Following the correct procedures by informing the DSL or Business Manager if they need to bypass the filtering and monitoring systems for educational purposes
- When working with Pupils to monitor pupils screens at all times
- Working with the DSL to ensure that any online safety incidents, including those that they become aware of that occur outside school are recorded correctly as detailed in clause 12 and appendix 4 and dealt with appropriately in line with this policy and/or the school's child protection policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy and anti-bullying 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/Carers

Parents/Carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Read, understand, and support the Acceptable Use for Pupils Rules (appendix 1 and 1a)

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

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 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
- Relationships and sex education and health education in secondary schools

The School uses resources from SWGFL and the Twinkl scheme of work which continuously re visits online safety. It is also covered in the school's PSHE curriculum. In addition, there is an online safety focus week each academic year consisting of assemblies and focused activities.

The School recognises that teaching about safeguarding, including online safety, needs to be adapted for all our pupils, sometimes on an individual level, as well as those pupils who are vulnerable children or victims of abuse. The school adapts the curriculum to take into account the levels of all pupils to ensure they are given the opportunity to access all lessons.

At the appropriate stage and in the appropriate way depending on their needs and abilities, pupils will be taught the following during primary and secondary years:

During primary school pupils will be taught to:

- To use technology safely and respectfully, keeping personal information private
- To identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies
- To recognise acceptable and unacceptable behaviour
- To identify a range of ways to report concerns about content and contact
- 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

During secondary education, pupils will be taught:

- To understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- To recognise inappropriate content, contact and conduct, and know how to report concerns
- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns
- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours

- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

The safe use of social media and the internet will also be covered in other subjects where relevant.

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. This policy will also be shared with parents.

Online safety will also be covered during parents' evenings.

The school currently uses the Smoothwall system to filter and monitor online use.

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with 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 behaviour policy.)

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 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 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 and anti-bullying 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 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 or Deputy Head 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.
- 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 cooperation

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 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 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

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.

The school 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.

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

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.

7. Acceptable use of the internet in school

All, staff and volunteers are expected to read and agree (through the schools' elearning platform) to the acceptable use of the school's ICT systems and the internet (appendix 2). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

All pupils and parents are expected to read and agree to the acceptable use for pupils policy (appendix 1 and 1a). A copy of the computer and internet safety rules will be displayed in all classrooms for pupils.

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

We will monitor the websites visited by pupils, staff, volunteers, 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 agreement policy and Computer and Internet Safety rules in appendices 1 and 2.

8. Pupils using mobile devices in school

Pupils may bring mobile devices or electronics (including smart watches) into school. These must be turned off and signed into the school office on arrival and then they are locked away in the school office until the end of the day. Pupils are encouraged to sign their devices in and out themselves where possible, or a supporting adult may do this for them. The device will be collected by the pupil from the box outside of the office at the end of the school day and signed out by themselves or their supporting adult.

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. Passwords must:
    - Expire every 90 days
    - Cannot be any of the previous last 3 passwords
    - Be a minimum length of 8 characters
    - Meet complexity requirements, including being a combination of upper-case, lower-case letters, numbers and special characters and there are restrictions around being too similar to the username.
- 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 – 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.

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 EnablesIT or the Business Manager.

10. 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. 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 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 which 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 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
- 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 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 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.

The Management Team 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 and Recording arrangements

The DSL or Deputy DSL's or Business Manager log behaviour and safeguarding issues related to online safety in the following ways:

- Online safety or safeguarding incidents relating to pupils are recorded in line with the school's child protection and safeguarding policy and dealt with in line with this policy.
- Online safety incidents that arise through the school's monitoring system or those that relate to staff should be recorded using the online safety incident log (see appendix 4) and dealt with

appropriately in line with this policy and/or the school's child protection policy. An incident report log template can be viewed in appendix 4. The incident report log is stored securely in the Blue shared drive.

This policy will be reviewed annually by the Business Manager and DSL. At every review, the policy will be shared and agreed with the Management Team. The review (such as the one available here) 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.

13. Links with other policies

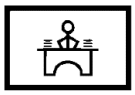
This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy
- Social Media Policy
- Mobile Phone and Smartwatch policy

Reviewed by:	Alex Labbett	**Date:** November 2023
Reviewed on:	April 2022. Replaces previous e-safety policy	
Last review on:	November 2022	
Next review on:	November 2024	

Appendix 1: Acceptable use agreement (pupils)

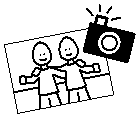
Computer, iPad and Internet Safety Rules

- Sign my personal device in and out of the office at the start and end of each day


- Ask an adult to use an electronic device or the internet before using

- Only use an electronic device or the internet when an adult is present

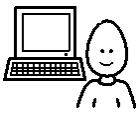


- Only film or take pictures with both the other person and an adult's consent


- Keep my username and password safe and do not share with others

- Tell an adult immediately if:
    - I click on a website by mistake
    - I receive messages from people I don't know
    - My friends or I received a message from someone I do know that has upset me
    - I find anything that may upset or harm me or my friends

- Be kind to others online and never rude (including bad language)



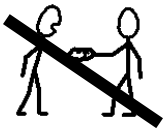

- Look after the school equipment and tell an adult straight away if something is broken or not working

- Never give my personal/private information (name, address or phone number) to anyone without permission of my teacher or parent/carer

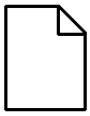
- Do not post pictures or school content online

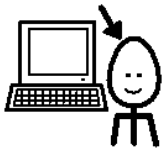
- The School will monitor computers, iPads and internet use

- Check with an adult before printing



- Never arrange to meet anyone offline without first consulting my parent/carer or without adult supervision





- Do not open attachments in emails or follow any links in emails without first checking with a teacher

- Save my work to the school network only

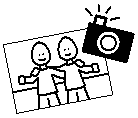
- Log off or shut down when I have finished using a device

Appendix 1a: Acceptable use agreement (pupils) (Limited Language)

- My device goes in and out of the office.


- Ask an adult to use a device or internet.

- An adult needs to be with you.



- Only film or take pictures when someone says its ok.


- Do not share my username and password with others.

- Tell an adult if:
    - I click on the wrong website
    - I get messages from people I don't know
    - I get messages that have upset me or my friends
    - I find anything that may upset or harm me or my friends

- Be kind to others online.


- Look after the school equipment. Tell an adult if something is broken or not working.

- Never give my information (name, address or phone number) to anyone without my teacher or parent/carer saying I can.

- Do not post pictures or school content online.

- The School will check computers, iPads and internet use

- Check with an adult before printing

- Do not arrange to meet anyone offline without talking to my parent/carer or without adult supervision

- Do not open attachments in emails or follow links in emails without checking with a teacher first

- Save my work to the school network only

- Log off or shut down when I have finished.

Appendix 2: Acceptable Use Policy (staff, volunteers and visitors)

1 **Introduction:** This policy sets out the requirements with which you must comply when using the School's IT and when otherwise using IT (including your own devices) in connection with your job including:

1.1 the School's email and internet services;

1.2 telephones;

1.3 the use of mobile technology on School premises or otherwise in the course of your employment (including 3G/4G/5G or Bluetooth or other wireless technologies) whether using a School or personal device (to include the use of Whatsapp and other technology based communications;

1.4 any hardware (such as laptops, printers or mobile phones) or software provided by, or made available by, the School or otherwise used in connection with your job; and

1.5 Any Artificial Intelligence software or technology made available to you by the School or otherwise used in connection with your role.

This policy also applies to your use of IT off school premises if the use involves Personal Data of any member of the School community or where the culture or reputation of the School are put at risk.

2 **Training: Induction training for new staff includes training on the School's online safety strategy. Ongoing staff development training includes training on technology safety together with specific safeguarding issues including sharing nudes and semi-nudes images and/or videos, cyberbullying, radicalistic and dealing with harmful online challenges and online hoaxes.**

3 **Failure to comply:** Failure to comply will constitute a disciplinary offence and will be dealt with under the School's Disciplinary Procedure.

4 **Property:** You must treat any property belonging to the School with respect and reasonable care and report any faults or breakages immediately to the Business Manager. You must not use the School's computers or other IT resources unless you are competent to do so and should ask for training if you need it.

5 **Viruses and other malicious code:** You should be aware of the potential damage that can be caused by computer viruses and other malicious code. You must not use, introduce or operate any hardware, programmes or data (including computer games) or open suspicious emails without permission from the Headteacher or Business Manager.

6 **Passwords**: Passwords should be long, for example, you could use a song lyric or a memorable phrase plus a number. Do not choose a password which is so complex that it's difficult to remember without writing it down. Your password should not be disclosed to anyone else. In addition:

6.1 Your password should be difficult to guess, for example, you could base your password on something memorable that no-one else would know. You should not use information which other people might know, or be able to find out, such as your address or your birthday.

6.2 You must not use a password which is used for another account. For example, you must not use your password for your private email address or online services for any school account.

6.3 Passwords (and any other security credential you are issued with such as a key fob or USB drive) must be kept secure and confidential and must not be shared with, or given to, anyone else. Passwords should not be written down.

7 **Leaving workstations:** If you leave your workstation for any period of time you should take appropriate action and, in particular, you should lock your screen to prevent access.

8 **Concerns:** You have a duty to report any concerns about the use of IT at the School to the Headteacher. For example, if you have a concern about IT security or pupils accessing inappropriate material.

9 **Online Platforms:** The School uses online platforms such as Zoom and Microsoft Teams to support and facilitate learning and pupil engagement. You must make sure that you follow the School's policies, procedures and instructions notified to you in respect of such platforms.

10 **Other policies:** This policy should be read alongside the following:

10.1 Code of Conduct;

10.2 Social media policy for staff;

10.3 Data Protection Policy for Staff;

10.4 Information Security Policy;

10.5 Acceptable use policy for pupils; and

10.6 Online safety policy, including the guidance it contains on the School's appropriate filtering and monitoring systems.

Internet

11 **Downloading:** Downloading of any programme or file which is not specifically related to your job is strictly prohibited.

12 **Personal use:** The School permits the incidental use of the internet so long as it is kept to a minimum and takes place substantially out of normal working hours. Use must not interfere with your work commitments (or those of others). Personal use is a privilege and not a right. If the School discovers that excessive periods of time have been spent on the internet provided by the School or it has been used for inappropriate purposes (as described in section 13 below), either in or outside working hours, disciplinary action may be taken and internet access may be withdrawn without notice at the discretion of the Director. Any personal use of a School device is subject to the School's permission in accordance with its policies. If you do use a School device for personal reasons, please be aware that such personal use may be monitored.

13 **Unsuitable material:** Viewing, retrieving or downloading of pornographic, terrorist or extremist material, or any other material which the School believes is unsuitable is strictly prohibited and constitutes gross misconduct. This includes such use at any time on the School's network, or via 3G or 4G or 5G when on School premises or otherwise in the course of your employment and whether or not on a School or personal device. Internet access may be withdrawn without notice at the discretion of the Head whilst allegations of unsuitable use are investigated by the School.

14 **Device syncing:** Personal use of School devices may result in the School device syncing with your personal accounts and devices, for example, if you log into a personal account on the School

device. This could, for example, result in private browsing history and personal information transferring from a personal device to a School device, and therefore becoming subject to monitoring by the School. You may be able to prevent this by turning off device syncing on your personal device. This is your responsibility and the School has no control over automatic syncing. If in doubt, do not use a School device for personal reasons.

15 **Location services**: The use of location services represents a risk to the personal safety of those within the School community, the School's security and its reputation. The use of any website or application, whether on a School or personal device, with the capability of publicly identifying the user's location while on School premises or otherwise in the course of employment is strictly prohibited at all times.

16 **Contracts:** You are not permitted to enter into any contract or subscription on the internet (including through an App) on behalf of the School, without specific permission from the Business Manager. This applies both to "free" and paid for contracts, subscriptions and Apps.

17 **Retention Periods**: the School keeps a record of staff browsing histories for a period of 90 days.

Email and other technology based communications

18 **Personal use of School systems:** The School permits the incidental use of its email systems to send personal emails as long as such use is kept to a minimum and takes place substantially out of normal working hours. Personal emails should be labelled 'personal' in the subject header. Use must not interfere with your work commitments (or those of others). Personal use is a privilege and not a right. The School may monitor your use of the email system, please see paragraphs 29 to 34 below, and staff should advise those they communicate with that such emails may be monitored. If the School discovers that you have breached these requirements, disciplinary action may be taken.

19 **Use of personal devices or accounts for School business**: the School accepts you may use your personal devices, social media or messaging services to maintain social contact with colleagues as part of your private life. Where contact with colleagues includes both personal and professional matters there is a risk of blurring boundaries as to what devices and platforms should be used for what type of contact. The School expects you to exercise your professional judgement in order to ensure all communication is appropriate and professional at all times. In the rare event you might need to contact a colleague about a work-related matter using a personal device or personal social media, you must keep any such messages brief and professional, and must not include any identifying and/or sensitive information. For example, you could send a message to a colleague's personal WhatsApp account asking them to check their School email account without providing any further information. All further communication should then take place using the appropriate School platform.

20 **Group communications**: Where necessary, the School permits the use of group communications, for example with the use of email groups or Whatsapp groups. When using such groups, staff should:

20.1 never share confidential personal details, particularly pupil or parent information;

20.2 not include pupils or parents in the group;

20.3 be mindful of the School's Dignity at Work Policy, Online Safety Policy, Social Media Policy and Staff Code of Conduct;

20.4 have no expectation that messages sent will remain private, for example the messages may be disclosable under a subject access request or may be used by the School in formal processes if they evidence misconduct or performance concerns; and

20.5 not use group messaging as a means of formal communication when an audit trail is needed.

21 **Status:** Email and other technology based communications (to include text or imessage or WhatAapp or any others, should be treated in the same way as any other form of written communication. Anything that is written in an email or other technology based communication is treated in the same way as any form of writing. You should not include anything in an email or technology based communication which is not appropriate to be published generally.

22 **Inappropriate use:** Any email message or other technology based communication which is abusive, discriminatory on grounds of sex, marital or civil partnership status, age, race, disability, sexual orientation or religious belief (or otherwise contrary to our Equal, Opportunities Policy), or defamatory is not permitted. Use of the email system in this way constitutes a breach of the School's harassment and bullying policy and may constitute gross misconduct. The School will take no responsibility for any offence caused by you as a result of downloading, viewing or forwarding inappropriate emails.

23 **Legal proceedings:** You should be aware that emails, texts and other messages are disclosable as evidence in court proceedings. This is the case regardless of whether the communication has taken place using the School's equipment and systems, or your own equipment and social media/messaging service. Even if messages are deleted, a copy may exist on a back-up system or other storage area.

24 **Jokes:** Trivial messages and jokes should not be sent or forwarded to the email system. They could cause the School's IT system to suffer delays and / or damage or could cause offence.

25 **Contracts:** Contractual commitments via an email correspondence are not allowed without the prior authorisation of the Director.

26 **Disclaimer:** All correspondence by email should contain the School's disclaimer.

27 **Data protection disclosures:** Subject to a number of limited exceptions, potentially all personal data about an individual may be disclosed should that individual make a subject access request under data protection legislation. There is no exemption for embarrassing information (for example, an exchange of emails containing gossip about the individual will usually be disclosable). **Staff must be aware that anything they put in an email or other message is potentially disclosable. This is the case regardless of whether the communication has taken place using the School's equipment and systems, or your own equipment and social media/messaging service.**

Artificial intelligence

28 **Artificial Intelligence:** The School wishes to support staff to use AI as a learning tool, in order to support pupils' learning, to boost productivity, and to help manage workloads efficiently and effectively. You are permitted to use named AI software at work and for work purposes. If you use AI technology at work or for work purposes, you must do so professionally at all times. This means that you may use AI as a tool to help you perform your role but must not use it to cut corners. You must not input any confidential information into free generative AI software such as ChatGPT. You must also check any output generated by AI technology before adapting it for your final use.

Monitoring

29 **Regular monitoring: The School** regularly monitors and accesses its IT system for purposes connected with the operation of the School. The School IT system includes any hardware, software, email account, computer, device or telephone provided by the School or used for School business. The School may also monitor staff use of the School telephone system and voicemail messages. Staff should be aware that the School may monitor the contents of a communication (such as the contents of an email).

30 **Purpose**: The purposes of such monitoring and accessing include:

30.1 to help the School with its day to day operations. For example, if a member of staff is on holiday or is off sick, their email account may be monitored in case any urgent emails are received; and

30.2 to check staff compliance with the School's policies and procedures and to help the School fulfil its legal obligations. For example, to investigate allegations that a member of staff has been using their email account to send abusive or inappropriate messages.

31 **Random monitoring:** Monitoring may be carried out on a random basis and it may be carried out in response to a specific incident or concern.

32 **Software:** The School also uses software which automatically monitors the School IT system (for example, it would raise an alert if a member of Staff visited a blocked website).

33 **Results of concern:** The monitoring is carried out by the Business Manager via Smoothwall. If anything of concern is revealed as a result of such monitoring then this information may be shared with Headteacher and Director In exceptional circumstances concerns may need to be referred to external agencies such as the Police.

Appendix 3: online safety training needs – self audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, and visitors?	
Are you familiar with the school's acceptable use agreement for pupils?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 4: online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**