Online safety policy

Swanbourne CE School

Mursley CE School

Drayton Parslow Village School

Kingfishers Pre-School (Mursley)

(In this policy known as the Three Schools)

Date adopted – **September 2023**

Date reviewed – **September 2025**

Date to be reviewed – September 2027

(Copies of this policy are available for staff, parents, visitors and volunteers on request from the school office).

Contents

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

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
- 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.

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The governing board

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

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

The governing board 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 board 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.

The governor who oversees online safety is Alison Terry.

All governors will:

- Ensure 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 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
- 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

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

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:

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the 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 ICT manager to make sure the appropriate systems and processes are in place
- Working with the, 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's child protection policy
- Ensuring that any online safety incidents are logged (see appendix 5) 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 (appendix 4 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 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.

3.4 The ICT manager (Turn It On)

The ICT 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
- 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 fortnightly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 5) 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 ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- 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 completing the Safeguarding Concern Form.
- Following the correct procedures by communicating with Turn It On, 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 (see appendix 5) 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'

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 ICT 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 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 primary schools have to teach:

- Relationships education and health education

In **Key Stage KS1**, 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 KS2** 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.

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/carers.

Online safety will also be covered during parents' information evenings.

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

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 1 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.

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.

The school also sends information/leaflets 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.

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 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 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 DSL.
- 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 DSL 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 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 Three Schools 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.

The Three Schools will treat any use of AI to bully pupils in line with our Anto-Bullying 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 Three Schools.

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 ICT systems and the internet (appendices 1 to 3). 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 to 3.

8. Pupils using mobile devices in school

Pupils are not permitted to bring personal devices into school.

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

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 3.

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 Turn It On. They must also inform the DSL.

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 Behaviour and Acceptable Use 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 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 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 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 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. An incident report log can be found in appendix 5.

This policy will be reviewed every year by the DSL or Deputy. At every review, the policy will be shared with the governing board. The review will be conducted alongside Turn It On, as the leaders in this field. They will advise as they are at the forefront of technology developments and are aware of the risks and harms related to it, especially how it evolves and changes rapidly.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff code of conduct
- Data protection policy and privacy notices
- Complaints procedure
- Acceptable use policy

Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

KS1 Internet and e-mail code of practice for pupils

Digital technology is an integral part of learning and life in the modern world. The internet can be a wonderful tool, if used appropriately and these rules are deigned to help us keep everyone safe keep and help us to be fair to others.

Early Years and KS1 pupils

- I will only use the internet as directed by my teachers.
- I will only search the internet using recommended 'safe search' apps/websites.
- I will not share passwords with other people.
- I will tell my teacher if I see something that is upsetting.
- I will not share any personal information online.
- I will not say unkind things about other people online.

I have discussed this with my child.

Signed: ……..……Parent/Guardian/Carer Date: ……

Appendix 2: KS2 acceptable use agreement (pupils and parents/carers)

KS2 Internet and e-mail code of practice for pupils

Please read this document carefully. Only once it has been signed and returned will access to the Internet be permitted. If any student violates these provisions, access to the Internet will be denied and the student will be subject to disciplinary action. Additional action may be taken by the school in line with existing policy regarding school behaviour. For serious violations, suspension or expulsion may be imposed. Where appropriate, police may be involved or other legal action taken.

I will
- only use the internet when supervised by a teacher or adult.
- never tell anyone I meet on the internet my home address, my phone number or my school's name, unless my teacher specifically gives me permission.
- never send anyone my picture without permission from my teacher/parents/carer.
- switch off the screen and tell the teacher if I see anything that makes me feel uncomfortable.
- never give my password to anyone and I will log off when I have finished using the computer.
- never arrange to meet anyone in person without first agreeing it with my parents/teacher/carer and get them to come along to the first meeting.
- never hang around in an Internet chat room if someone says or writes something which makes me feel uncomfortable or worried, and I will always report it to a teacher or parent.
- never respond to unpleasant, suggestive or bullying e-mails or bulletin boards and I will always report it to a teacher or parent.
- not look for bad language or distasteful images while I'm online and I will report bad language or distasteful images to a teacher or parent if I come across them accidentally.
- always be myself and will not pretend to be anyone or anything I am not.
- not use e-mail to send or encourage material which is pornographic, illegal, offensive or annoying or invades another person's privacy
- not download software from the Internet (including screen savers, games, video clips, audio clips etc).

I know that
- the contents of my e-mail and the sites I visit will be monitored by the Network Manager
- information on the Internet may not always be reliable and sources may need checking.
- the posting of anonymous messages and the forwarding of chain messages is not allowed.

I understand
- I can access only sites and material relevant to my work in school and that I will not be able to use the Internet if I deliberately look at unsuitable material.
- I will not be able to use the Internet if I deliberately hack into the schools' or other systems.

I/we have read and have discussed the code with our son/daughter and agree to support the school's policy on the use of the Internet.

Signed: ……..……Parent/Guardian/Carer Date: ……

Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors)

Acceptable Use Policy for Adults

(Teaching Staff, Non-Teaching Staff and Volunteers)

Swanbourne CE School

Mursley CE School

Drayton Parslow Village School

Kingfishers Pre-School (Mursley)

(In this policy known as the Three Schools)

This policy was adopted on – **September 2023**

The policy was reviewed by – **September 2025**

The policy is to be reviewed by – **September 2027**

(Copies of this policy are available for staff, parents, visitors and volunteers on request from the school office).

Key Points of our Acceptable Use Policy (AUP) for Adults

The Three Schools have provided computers/IPads for use by staff as an important tool for teaching, learning and administration of the school. Use of school computers/IPads, by both members of staff and pupils, is governed at all times by the following policy. Please ensure that you understand your responsibilities under this policy, and direct any questions or concerns to the Head Teacher in the first instance.

The purpose of the policy is to ensure the school network is operated safely and all users of ICT are safe. It refers to our school ICT network and to the use of mobile technologies within it and explains the behaviours, which are acceptable and unacceptable within our school.

This document outlines the key points of our AUP. It has been written to ensure all adults working within school are aware of the rules, risks and procedures we operate under our full AUP, which is located on our ICT system.

All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. Our AUP must be fully complied with at all times. All users of the school network should note that it is monitored on a regular basis. Any person who is found to have misused the school system or not followed our AUP could face the following consequences:

- Temporary or permanent withdrawal from the school system
- Suspension or exclusion from the school
- Disciplinary action
- In the most serious cases legal action may also be taken.

Whilst our network and systems are organised to maintain the most secure environment possible it is **your responsibility to make sure the children you are directly working with are safe.** All adults working in school must do so under the guidance of the member of staff to whom they are responsible.

As an adult working in school you may be the first point of contact in dealing with incidents of ICT misuse or abuse. Every such incident must be reported to the Head Teacher who will then follow the procedures set out in our AUP.

Your key responsibilities are:

- Maintaining an appropriate level of professional conduct in your own internet use within school.
- Developing and maintaining knowledge of internet safety issues, particularly with regard to how they might affect children.
- Implementing our school AUP through effective classroom practice.
- Reporting any instances of ICT misuse to the Head Teacher.
- Supporting pupils who experience problems when using the internet, working with the Class Teacher.
- Using the internet and ICT facilities to ensure that internet safety is not compromised e.g. evaluating websites in advance of classroom use, using chid oriented search engines.
- Embedding internet safety messages wherever possible.
- Following the school rules relating to acceptable use of our ICT equipment and other mobile technologies.
- Copies of our rules for pupil use of the network are displayed around the school. Please ensure you have read them and make sure the pupils you work with adhere to them.

School ICT Network

The school Network and associated services may be used for lawful purposes only.

Passwords

- Each child and adult working within the school must log on to the computers using the username and password given to them (class account or individual account).
- Passwords need to be kept a secret. Both adults and children need to fill in appropriate class computer logs, stating what time they logged onto the computer and what time they logged off. If for any reason a child or adult needs to leave their computer, they have to lock the computer to prevent others from using their account by pressing 'Ctrl, Alt and Delete'.
- It is forbidden to use other children's/adult's/class accounts or files. Both adults and children will respect copyright and not copy anyone's work and call it their own.

- **For the children in our school who are unable to understand the 'Internet and Email Code of Practice for Pupils' and for the children who are unable to log in and log off using their own password, the adult(s) working with those children will take full responsibility for their safe internet use in school.**
- Any supply teachers or visitors to the school must request laptop access details and passwords to be supplied by the class teacher or Teaching Assistant. This information will need to be kept confidential and used on the appropriate class computer for the class they are teaching.

Software and Downloads

- All users of the network must virus check any USB device storage devices before using on the network.
- All users are prohibited from installing software onto the network from a CD-ROM, other device or by downloading from the Internet without permission from the ICT Technician (Turn IT On). If users need a new program installing onto the computer, our ICT Technician will be asked to do this if possible.
- Copyright and intellectual property rights must be respected when downloading from the internet.

Personal Use

- The Three Schools recognise that occasional personal use of the school's computer is beneficial both to the development of ICT skills and for maintaining a positive work-life balance. Such use is permitted, with the conditions that such use:
- Most comply with all other conditions of the AUP as they apply to non-personal use, and all other school policies regarding staff conduct.
- Must not interfere in any way with your other duties or those of any other member of staff.
- Must not have any undue effect on the performance of the computer system; and
- Must not be for any commercial purpose or gain unless explicitly authorised by the school.

Personal use is permitted at the discretion of the school and can be limited or revoked at any time.

Email

- All members of staff are provided with a school email address for communication both internally and with other email users outside of school.
- No member of staff (including governors and non-teaching staff) must use non-school email accounts for any school/work related activity – No exceptions!
- Users are responsible for e-mail they send and should be aware that these are open to be read and should be treated as public.
- All members of staff should be aware that email is not guaranteed to be private. Messages relating to or in support of illegal activities will be reported to the authorities. Anonymous messages are not permitted.
- E-mail should be written carefully and politely and should never contain anything which is likely to cause annoyance, inconvenience or needless anxiety. Anonymous messages and chain letters must not be sent.
- When writing emails, you should use appropriate language. You should not use language that could be calculated to incite hatred against ethnic, religious or other minority. You need to remember that you are a representative of the school on a global public system. Illegal activities of any kind are strictly forbidden.
- All emails both sent and received will be scanned by forensic software.
- E-mail attachments should only be opened if the source is known and trusted.
- Children are not permitted under any circumstances to e-mail a member of staff using their personal e-mail address. In addition, members of staff should not be emailing children using their personal email address.
- Privacy – Staff are not to reveal any personal information (e.g. name, address, age, telephone number, social network details) of other users to any unauthorised person. Staff will not reveal any of their personal information to the pupils.Staff will not trespass into other users' files or folders.
- Staff will ensure that all login credentials (including passwords) are not shared with any other individuals, displayed or used by any individual than myself. Likewise, staff are not to share those of other users. Staff need to ensure that if they I think someone has learned their password then they will change it immediately and/or contact ICT technician. Staff will ensure that they log off after their session has finished. If they find an unattended machine logged on under another username they will not continue using the machine – Staff should ensure they log it off immediately.
- **Any unsuitable communications received must be reported to a member of staff immediately.**

Images/Videos

- All children need parental permission to have photographs or videos published electronically or in a public area even if they are unidentifiable.
- No photos or videos which include nudity or inappropriate actions are permitted to be taken or downloaded under any circumstance.

Network Protocol

- School computer and Internet use must be appropriate to a pupil's education or to staff professional activity.
- Respect other people's material and do not corrupt, interfere with or destroy them.
- Do not open other people's files without expressed permission.
- When working with personal data ensure that the data is secure.

Internet Usage

- Pupils must be supervised at all times when using the internet.
- Activities should be planned so 'open searching' is kept to a minimum. The facility for caching sites should be used prior to using the internet with pupils.
- When searching the internet with pupils, adults should encourage the children to use 'child safe' search engines. However safe search is set on all computers in school as a default on search engines.
- The use of social networking sites, public chat rooms and messaging systems (e.g. Facebook, Messenger, Twitter) is not allowed in school.
- Use the internet for personal financial gain, gambling, political purposes or advertising is forbidden.
- Staff will not attempt to visit websites that may be considered inappropriate or illegal.
- Staff are aware that downloading some material is illegal and that the police or other authorities may be called to investigate.

Use of Social Networking Sites and Online Forums

Staff must take care when using websites such as Facebook, Twitter, Dating Sites etc, even when such use occurs in their own time their own computer at home. Social Networking sites invite users to participate in informal ways that can leave you open to abuse, and often make little or no distinction between adult users and children.

Staff must not allow any pupil to access personal information you post on a social networking site. In particular:

- Staff must not add a pupil to their 'Friends list', nor invite them to be friends with them.
- Staff must ensure that personal information is not accessible via 'Public' setting, but ensure it is to a 'Friends only' level of visibility.
- Staff should avoid contacting any pupil privately via social networking site, even for school-related purposes.
- Staff should take steps to ensure that any person contacting them via a social networking website is who they claim to be, and not an imposter, before allowing them to access to their personal information.

It is advised not to accept invitations from the pupils' parents or carers to add staff as a 'friend' to their social networking sites, nor should staff invite them to be their friends. Damage to professional reputations can inadvertently be caused by quite innocent postings or images. Staff will need to ensure that any private social networking sites/blogs that they create or actively contribute to are not to be confused with their professional role in anyway.

Staff should also take care when posting to any public website (including online discussion forums or blogs) that their comments do not harm their professional standing or the reputation of the school – even if their online activities are entirely unrelated to the school.

- Unless authorised to do so, you must not post comments on websites that may appear as if you are speaking for the school.
- You should not post any material online that can be clearly linked to the school that may damage the school's reputation.
- You should avoid posting any material clearly identifying yourself, another member of staff, or a pupil, that could potentially be used to embarrass, harass or defame the subject.

Use of your own Equipment

- Any mains-operated personal computer or electrical equipment brought on site, for any use, is subject to a Portable Appliance Test (PAT) by site maintenance staff, and must not be used until approved. This test must be performed at regular intervals as required by school's normal rules on electrical safety testing (PAT is completed on an annual basis).
- You must not connect personal computer equipment to school computer equipment without prior approval from ICT Technician (Turn IT On), without the exception of storage devices such as USB memory sticks.

Mobile Devices

- Personal mobile phones should not be used in areas of school where pupils have access.
- During teaching time, mobile phones should be turned off or put on silent mode and stored in a cupboard, locker or bag away from the children.
- Adult are allowed to access their personal phones on breaks, lunch times and after school in designated areas e.g. staff room or teachers classroom (safe, suitable places - Where pupils are not present).
- It is forbidden to take photographs/videos of pupils on personal mobile phones.
- No images of the children should be taken without parental consent and permission from a member of staff using any mobile device e.g. phones, school cameras. These devices must not be removed from the school premises if they contain images of pupils and without permission from a member of staff.

Supervision of Pupil Use

- **Pupils must be supervised at all times** when using school computer equipment.
- When arranging use of computer facilities for pupils, staff must ensure supervision is available.
- Supervising staff are responsible for ensuring that the separate Internet and Email Code of Practice for Pupils is enforced.
- Supervising staff must ensure they have read and understand the separate guidelines on E-safety, which pertains to the Child Protection issues of computer use by pupils.

Reporting Problems with the Computer System

It is the job of the ICT Network Manager (Turn IT On) to ensure that the school computer system is working optimally at all times and that any faults are rectified as soon as possible.

- You should report any problems that need attention to ICT Technician (Turn IT On).
- If you suspect your computer has been affected by a virus or other malware, you must report this to ICT Technician (Turn IT On) immediately.
- If you have lost documents or files, you should report this as soon as possible. The longer a data loss problem goes unreported, the less chances of your data being recoverable.

Reporting Breaches of this Policy

All members of staff have a duty to ensure this Acceptable Use Policy is followed. You must immediately inform the ICT Technician (Turn IT On) or the Head Teacher, of abuse of any part of the computer system. In particular, you should report:

- Any websites accessible from within school that you feel are unsuitable for staff or pupil consumption
- Any inappropriate content suspected to be stored on the computer system. This may be contained in email, documents, pictures, etc.
- Any breaches, or attempted breaches, of computer security, or
- Any instance of bullying or harassment suffered by you, another member of staff, or a pupil via the school computer system. All reports will be treated confidentially.

Electronic Devices - Searching & Deletion

In accordance to 'The Education Act 2012' school has the right to search and or delete anything from personal devices if they believe illegal or suspicious activity is taken place.

Exemptions

All the above stands unless given permission from the Head Teacher e.g. while on residential trips, permission may be given to designated staff to upload photos onto our Class Dojo, School Facebook or Twitter account.

Review and Evaluation

This policy will be reviewed regularly and in response to any changes affecting the basis of the original risk assessment, for example: significant security incidents, new vulnerabilities and significant changes to the organisation or technical infrastructure. Changes to this policy will be communicated to all staff. Our Acceptable Use Policy (AUP) has been created by our school governors and senior managers and approved by the whole school community.

I have read, understood and agree to comply with the AUP:

Signed: …… Date: ……

Print Name: ……

Position in School: ……

Appendix 4: 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, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents/carers?	
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 5: 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**