The Unity of Titchmarsh, Warmington and Nassington Schools

E-Safety and Acceptable Use Policy

1. Aims and Objectives

- Our aim is for staff and pupils to safely use ICT and the Internet to enhance teaching and learning in an appropriate and safe manner.
- Access to the Internet is necessary to fulfil the requirements of the National Curriculum. At Foundation Stage, the majority of access to the Internet will be by adult demonstration or close supervision of a specific website. At Key Stage One, pupils will have supervised access to specific approved sites. At Key Stage Two, independent Internet access forms part of the Curriculum, following education in responsible and appropriate use.
- Staff will have open, but monitored, Internet access for research purposes, lesson planning, continued professional development and professional communication.
- All staff and any other adults involved in supervising children accessing the Internet will be provided with this Policy and will have its importance explained to them. All staff receive acceptable use policies regarding use of ICT in school and any assigned hardware as part of the induction pack for each year along with the Code of Conduct. E-safety will form part of staff training through briefings and Unity meetings.
- All parents (and pupils from Key Stage One onwards) will be provided with 'Rules for Responsible Internet Use' and will be required to sign to say they agree with these rules before their child has Internet access. Inappropriate use will be considered a disciplinary issue.

The National Curriculum states that children must 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 technologies".

Additionally, the Unity has, in reviewing this policy, used 'Teaching Online Safety at School' (June 2019) to ensure curriculum content covers the recommended guidance regarding:

- Evaluating what pupils see online
- Acceptable online behaviour
- How and where to seek support
- Health and well-being.

Recognising techniques for persuasion
Identifying online risks
Safe navigation and management of information

2. E-safety

E-safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and pupils, encouraged by education and made explicit by published policies and rules.
- Sound implementation of the E-safety policy in both administration and curriculum.
- Safe and secure broadband.

E-safety lessons are delivered to every year group with continuous reminders. The following measures are also implemented:

- Staff will check that sites pre-selected for pupil use are appropriate to the age and maturity of pupils.
- Staff will be particularly vigilant when pupils are undertaking their own Internet research.
- The 'Rules for Responsible Internet Use' will be displayed in classrooms.

Should material deemed inappropriate be viewed, the following measures are in place:

- A most important element of our 'Rules for Responsible Internet Use' is that pupils will be taught to tell a teacher **immediately** if they encounter any material that makes them feel uncomfortable.

Links with Service Six, NSPCC and Blue Butterfly (Northants Police) ensure annual classroom sessions on e-Safety from external providers and similar workshops for parents and carers.

- If there is an incident in which a pupil is exposed to offensive or upsetting material the school will respond to the situation quickly and on a number of levels. Responsibility for handling incidents involving children will be taken by the Computing Co-ordinator /technician and the DSL in consultation the Executive Headteacher and the pupil's class teacher. All the teaching staff will be made aware of the incident at a Staff Meeting if appropriate.

- If one or more pupils discover (view) inappropriate material our first priority will be to give them appropriate support. The pupil's parents/carers will be informed and given an explanation of the course of action the school has taken. The school aims to work with parents/carers and pupils to resolve any issue.

- If staff or pupils discover unsuitable sites the Computing Co-ordinator / technician will be informed. The Computing Co-ordinator /ICT Technician will report the URL address and content to the Internet Service Provider and the LA; if it is thought that the material is illegal, after consultation with the ISP and the LA, the site will be referred to the Internet Watch Foundation and the police.

- Complaints of a child protection nature will be dealt with in accordance with the school's child protection procedures.

- Pupils are expected to play their part in reducing the risk of viewing inappropriate material by obeying the 'Rules for Responsible Internet Use' which have been designed to help protect them from exposure to Internet sites carrying offensive material. If pupils abuse the privileges of access to the Internet or use of email facilities, then sanctions consistent with our School Behaviour Policy will be applied. This will involve informing the parents/carers. Teachers may also consider whether access to the Internet may be denied for a period.

3. Broadband Services

Our Broadband provider provides a 'firewall' filtering system to prevent access to material deemed inappropriate for children. Additional 'application control' filtering is in place to ensure safe and secure use of Internet through portable devices, such as iPads. Pupils will be made aware that, as 'Computer Partners', they are both responsible for the search content and should take responsibility and tell an adult if they are unhappy about anything their partner is accessing. Generic logins are in place for access to computers but not to specific programs such as Teams, Purple Mash or MyMaths where pupils have individual accounts.

The individual school will provide encrypted data sticks or hard drives for teaching staff use to minimise use of own devices and to limit potential data breaches.

Weekly reports are provided by the Service Provider to detail online searches – these are sent to the ICT Technician, Office Manager and Executive Headteacher for checking and actioning. Where there are concerns, these will be checked by the Executive Headteacher and, if required, will be dealt with according to the Code of Conduct. These are also available for checking by the Safeguarding Governors.

4. Maintaining the Security of the School ICT Network

We are aware that connection to the Internet significantly increases risk that a computer or a computer network may be infected by a virus or accessed by unauthorised persons.

The ICT Technician will ensure that virus protection software is up-dated regularly and will keep up-to-date with new IT development. She/he will work with the LA and Internet Service Provider to ensure system security strategies to protect the integrity of the network are improved, as and when necessary.

Neither staff nor pupils will install software or hardware brought in from an outside source on any computer. Any memory stick, or other media for transferring data, used between two or more computers will be scanned for viruses on insertion. All staff laptops and PCs have passwords to protect data and any memory sticks/hard drives taken off-site must be encrypted. Practice is in line with GDPR regulations. For Nassington, Windows BitLocker is being used to ensure encryption is in place for any portable devices

5. Using Email

KS2 pupils will learn how to use an email application and be taught email conventions. Staff will be provided with school email addresses for communicating with colleagues. For the purpose of remote learning during school closure or lockdown, pupils will have a school email to use which can only be used internally within the school email system. Additionally, any emails sent have to be approved by a staff member, therefore providing additional safety and safeguards.

It is important that communications with persons and organisations are properly managed to ensure appropriate educational use and that the good name of the school is maintained.

For work-life balance and security, staff are encouraged NOT to have email-based apps on their personal devices. Where they do, the device must be passcode protected and passwords must be used to access emails to ensure an additional level of security. Erasure facilities should also be activated on the relevant device.

Therefore:

- Pupils will taught to use email in conjunction with the 'Rules for Responsible Internet Use';
- Teachers will reinforce these rules as they monitor children learning about email.
- When learning about email and formatting their school accounts, children will be reminded not to attach personal photographs or include personal details, such as their home address and telephone number. They should never arrange to meet anyone.

6. Using a Web Browser

Pupils are taught to use suitable web search engines, such as Google and Junior Safesearch. Staff and pupils use the Internet to find and evaluate information. Access to the Internet is a planned part of the curriculum that will enrich and extend learning activities and will be integrated across all subjects.

As in other areas of their work, we recognise that pupils learn most effectively when they are given clear objectives for Internet use.

Different ways of accessing information from the Internet will be used depending upon the nature of the material being accessed and the age of the pupils:

- access to the Internet may be by teacher (or sometimes other adult) demonstration;
- pupils may be given a suitable web page or a single web site to access;
- pupils may be provided with lists of relevant and suitable web sites which they may access;
- older, more experienced, pupils may be allowed to undertake their own Internet search; pupils will be expected to observe the 'Rules for Responsible Internet Use' and will be informed that checks can and will be made on files held on the system and the sites they access.

Pupils accessing the Internet will be supervised / guided by an adult at all times. They will only be allowed to use the Internet once they have been taught the 'Rules for Responsible Internet Use' and parents have signed to acknowledge these rules.

7. Internet Access and Home/School Links

Parents will be required to sign the 'Rules for Responsible Internet Use' and should promote these rules during home Internet usage. When use of ICT or the Internet is required as part of homework, children should continue to abide by the 'Rules for Responsible Internet Use'. If there is no ICT access at home, parents should speak to the Computing Coordinator / class teacher for school access to be made available.

8. Using Information from the Internet

We believe that, in order to use information from the Internet effectively, it is important for pupils to develop an understanding of the nature of the Internet and the information available on it. In particular, they should know that, unlike the school library for example, most of the information on the Internet is intended for an adult audience, much of the information on the Internet is not properly audited/edited and most of it is copyright.

- pupils will be taught to expect a wider range of content, both in level and in audience, than is found in the school library or on TV;
- teachers will ensure that pupils are aware of the need to validate information whenever possible before accepting that it is true, and understand that this is even more important when considering information from the Internet (as a non-moderated medium);
- when copying materials from the Web, pupils will be taught to observe copyright;
- pupils will be made aware that the writer of an email or the author of a web page may not be the person claimed.

9. Publishing pupils' images & social networking

Pupils' work and photographs of pupils' learning activities may be published to the School Website, Class Dojo (where applicable), blogs or on occasion to local press sites in accordance with parental consent and general sensitivity
.

Parents and staff are not permitted to publish photographs or video of any child other than their own on social networking sites or other forms of media. This information will be communicated to parents via school newsletters and by senior staff at school events

Any comments posted on Internet forums or social networking sites pertaining to the school should be respectful to the children, staff and reputation of the school.

Social networking sites are blocked by the broadband filtering and are not permitted to be used in school by staff or pupils, without prior consent from the Executive Headteacher or Computing Co-ordinator for the purpose of education only.

Pupils are not permitted to bring portable devices, such as mobile phones to school. Any non-compliance will be dealt with in accordance with the school's Behaviour Policy.

10. "Sexting" and Nude and Semi-Nude Images

Sexting is to be viewed as an unwanted consequence of access to technology. The reality is that mobile technology and social networking is a constant pressure in young people's lives so banning technology is not a solution. Sexting needs to be seen as part of a wider picture which has received a lot of media attention and has been called the sexualisation of children. This includes issues such as pornography and gender based bullying and coercive sexual pressures placed on young people and as such, is a safeguarding and child protection issue. It is to be treated with the utmost urgency and as such be dealt with swiftly. Dependent upon the severity and nature of the texts, the matter should be handled sensitively yet comprehensively involving both sets of parents involved - both the instigators and the recipients in the first instance to alert them to the dangers and the possibility of a referral to the police and social services. If it does not cease immediately then a referral to the local safeguarding board (MASH team) should be considered.

The same approach should be used in relation to nude and semi-nude images – all staff have received updates regarding this in their Safeguarding Training. Additionally, the Unity issues an updated copy of Keeping Children Safe in Education each year and an updated Safeguarding policy which provides further advice.

11. Cyberbullying

Any behaviour that is rude, threatening or harmful and takes place online will not be tolerated. The same expectations of behaviour in school apply to the online world. Email accounts will be frozen if an episode of cyber bullying takes place until the incident can be fully investigated. Individuals found to be bullying other pupils or staff online will be suspended from all online activity and dealt with in accordance with the school's Behaviour Policy. Additionally, any inappropriate online posts made by staff or parents must be reported to the Executive Headteacher. Any inappropriate posts made by the Executive Headteacher must be reported to the Chair of Governors.

It may be appropriate to deal with cyberbullying in line with the 'child-on-child abuse' guidance as detailed in our Safeguarding Policy.

12. Physical security and wilful damage

Staff users are expected to ensure that portable ICT equipment, such as laptops and iPads are securely locked away or concealed when not in use. Items taken off the school premises are done so in accordance with the agreement of issue (iPads) and the same rules apply for laptops. Any loss or damage should be reported immediately to the Computing Coordinator / Executive Headteacher. An up-to-date audit needs to be kept of portable ICT equipment that is assigned to staff.

It is an expectation of the Unity that iPads and laptops are plugged in and secured at the end of each day. Items to be taken off-site must be done so only with the express permission of the Executive Headteacher.
Any malicious attempt to harm or destroy any equipment or data of another user or network connected to the school system will result in loss of access, disciplinary action and, if appropriate, legal referral. This includes the creation or uploading of computer viruses. The use of software from unauthorised sources is prohibited.

13. Acceptable Online Behaviour

Staff personal conduct online should be of the same high standards expected in school and colleagues are reminded of the Unity Code of Conduct. Staff should ensure that, should they use social media, they regularly check their privacy settings are up to date and that they are mindful of what they post or comment on whilst using social media. They must ensure that they do not post anything that might bring themselves or the Unity into disrepute and, if they believe that they have breached such guidelines, inform the Executive Headteacher immediately. Staff should also be mindful when using CHAT GTP or other artificial intelligence applications and must not use any school-related data as this will be permanently uploaded to any application and is a breach of GDPR.

Staff should also:

- ensure that they password-protect their computers and ensure that equipment is not left unattended at any time;
- ensure that a sleep facility is in place for their PC to prevent others from looking on their computer;
- ensure that they use a Unity-provided encrypted memory stick to transport any data to and from school and that material is saved only on the stick provided to reduce potential data breaches (or use One Drive);
- be mindful that any data they use and save may be accessed by the subject so professional guidelines should be used at all times;
- be mindful of data security – for example, displaying information in an easily accessible place, an unlocked office or window;
- ensure that they return the memory stick on termination of employment and check with the Executive Headteacher regarding any documents (e.g. planning, teaching resources) they may wish to take with them;
- ensure that any data used at home is subject to the same levels of scrutiny so security measures should be in place to ensure data safety. It is recommended that staff save to their encrypted sticks to ensure data security levels are as high as possible.

Staff are reminded that they should not use personal devices to take pictures of the pupils. iPads and cameras are provided by the school for this purpose. Breach of this will be treated as potential gross misconduct. Where the staff member is a parent of a child in school, they should follow the usual permission procedures. Again, failure to do this may be treated as a disciplinary matter.

During remote learning sessions, staff must remain professional at all times. For remote learning sessions led by a staff member from home, an additional staff member must be online to provide support and for safeguarding purposes. If remote learning is being led from school during a school day, an open door policy will operate and senior staff will regularly visit classes to quality assure proceedings.

Pupils breaking the online safety agreements will be reported to the Online Safety Lead (Executive Headteacher) who will undertake an investigation and will follow the appropriate behaviour and safeguarding procedures. A log of these will be kept centrally.

14. Health and Safety & Risk Assessment

Teachers will ensure that children work in a safe environment with regard for health and safety regulations. In our experience the measures set out in this policy have been highly effective. However, due to the international scale and linked nature of information available via the Internet, it is not possible to guarantee that particular types of material will never appear on the computer screen. Neither the school nor the LA can accept liability for the material accessed or any consequences thereof.

15. Equal Opportunities

We have carefully considered and analysed the impact of this policy on equality and the possible implications for pupils with protected characteristics, as part of our commitment to meet the Public Sector Equality Duty requirement to have due regard to the need to eliminate discrimination, advance equality of opportunity and foster good relations.

16. Special Educational Needs

We aim to provide suitably differentiated opportunities which are challenging, achievable, and are supported by resources and expertise appropriate to the child's individual requirements.

17. Monitoring, Evaluation and Review

The Governing body will review this policy and assess its implementation and effectiveness. The policy will be shared with all staff via the shared area and be available to parents on the school website. The policy will be implemented under the guidance of the Computing Coordinator /ICT Technician and the Executive Headteacher.

Appendix A: Online Safety

NOTE

Please see paragraph from Keeping Children Safe in Education (2023) here.

138. Online safety and the school or college's approach to it should be reflected in the child protection policy. Considering the 4Cs will provide the basis of an effective online policy. The school or college should have a clear policy on the use of mobile and smart technology. Amongst other things this will reflect the fact many children have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G). This access means some children, whilst at school or college, sexually harass, bully, and control others via their mobile and smart technology, share indecent images consensually and non-consensually (often via large chat groups) and view and share pornography and other harmful content. Schools and colleges should carefully consider how this is managed on their premises and reflect this in their mobile and smart technology policy and their child protection policy.

Teaching pupils to stay safe online and keeping children safe online in school is a crucial part of safeguarding. It is essential that children are safeguarded from potentially harmful and inappropriate online material. We take a whole school approach to online to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

Our approach to online safety runs through every aspect of our work with children, including (but not limited to):

- curriculum planning and RSHE;
- teacher training;
- the role and responsibilities of the designated safeguarding lead; and
- parental engagement.

This appendix complements and should be read alongside our Online Safety policy. Staff must read the Online Safety Policy in conjunction with our Code of Conduct in relation to personal online behaviour. All staff receive online safety training at induction, with regular updates and formal annual training thereafter.

The Designated Safeguarding Lead (DSL) takes lead responsibility for online safety. The DSL attends training regularly to ensure that they understand the unique risks associated with online safety and to ensure that they are confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online at school.

The Executive Headteacher takes lead responsibility for online safety and understanding the filtering and monitoring systems and processes in place. The DSL team attend training regularly to ensure that they understand the unique risks associated with online safety and to ensure that they are confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online at school.

Risks to children

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

- **content**: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- **contact**: being subjected to harmful online interaction with other users; for example: 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; for example, 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.

We refer to these four areas of risk when planning our approach to online safety and ensuring that we are safeguarding children against a broad spectrum of potential online harms.

Filtering and monitoring

Our filtering and monitoring procedures, including our review process, are informed by the DfE guidance manual '**Meeting digital and technology standards in schools and colleges**'[1]. For more information about the filtering and monitoring standards we adhere to, see '**Filtering and monitoring standards for schools and colleges**' (March 2022).[2]

In order to keep children safe when using school IT equipment, we ensure that all devices are linked to the school network and the highest level of filtering is in place. This is regularly reviewed by our peripatetic IT technician. Pupils are regularly reminded when using IT equipment of how to use it responsibly and what to do if they are concerned in any way about its use. The Executive Headteacher and IT Technician receive weekly updates regarding filter use and real-time alerts. Any serious breach of these systems will be treated in line with our disciplinary procedures.

[1] **https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges**

[2] **https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-standards-for-schools-and-colleges**

Staff devices can only be used in line with GDPR regulations and encrypted memory sticks are provided to ensure that sensitive data cannot be stored on staff devices.

We are mindful that “over-blocking” can lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding and mitigate against this by teaching pupils how to use the internet safely and monitoring them while they are using it. The appropriateness of any filters and monitoring systems are a matter for will be informed in part, by the risk assessment required by the Prevent Duty.

Pupil mobile phones

Pupils are not allowed to have mobile phones in school except where there is a prescribed medical need e.g. diabetic monitoring .
See Section 12 of this policy for more details about staff use of mobile phones and smart technology.

Remote learning

When remote learning is being used, pupils use their school IT account which operates only within the school community. All emails and chats are monitored by staff and pupils are aware that any email they send has to be approved by a member of staff – this will then remove any risk of them being contacted by outside agencies as staff members have to approve the email before the pupil can read it.

Where remote learning is misused by pupils, accounts will be suspended and appropriate disciplinary action will be taken by staff.

Additionally, where remote learning is required, letters with clear guidance and expectations are sent to parents and carers with protocols and expectations outlined so that they are aware of the behaviour standards required.

How to report online safety concerns

If pupils, parents or staff have any concerns about online safety, or need to make a disclosure, they should speak to the Designated Safeguarding Lead or deputy without delay. The contact details for these members of staff can be found on the Safeguarding section of the website and Child Protection policy.

Cybersecurity

We ensure that we have the appropriate level of security protection procedures in place in order to safeguard systems, staff and children and we review the effectiveness of these procedures periodically to keep up with evolving cyber-crime technologies. This is informed by the DfE document ‘**Cyber security standards for schools and colleges**’.[3]

Regular review of our approach to online safety

We recognise that technology, and risks and harms related to it evolve and changes rapidly.
We carry out an annual review of our approach to online safety, supported by an annual risk assessment that considers and reflects the risks their children face. This is informed by local and national training, regular updates and the DfE guidance **‘Meeting digital and technology standards in schools and colleges’**.[4]

More information

For more information about online safety, please see Part 1 of Keeping Children Safe in Education (2023).

Associated Policies:

GDPR Policy
Staff Code of Conduct/Staff Handbook
Home-School Agreement
Child Protection/Safeguarding Policy Appendix F: Online Safety
Whistleblowing Policy
Disciplinary Policy

[3] **https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/cyber-security-standards-for-schools-and-colleges**

[4] **https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/cyber-security-standards-for-schools-and-colleges**

School Procedures for Parents to Sign Document
Teaching Online Safety in School (June 2019)
Relationships and Sex Education Policy
Purple Mash Computing Scheme of Work
Video and Photographic Use Policy

The Unity of Titchmarsh, Warmington and Nassington Schools

E-Safety and Acceptable Use Policy

Rules for Responsible Internet Use We use the school computers and the Internet connection to help our learning. These rules will help us to be fair to others. They will also help to keep everyone safe and the system secure.

Using the computers:

- I will login using the username and password that I have been given and always log off after I have finished working at a computer.
- I will not look at or interfere with other people's files.
- I will not bring in memory sticks, DVDs or CDs from outside school and try to use them on the school computers.
- I will not use portable devices (such as phones and ipods etc.) during the school day.
- I will treat all ICT equipment with care and respect and will inform an adult immediately if any damage occurs.

Using the Internet:

- I will only use the Internet when given permission by a teacher as part of my work.
- I will not access any link or search for anything online that I know or think would be considered unacceptable by my teachers.
- I will not use Internet chat rooms or any other form of social networking.
- I will not download games, music or other files from the Internet without permission.
- I will not complete and send forms without permission from my teacher.
- I know that the school may check my computer files and may monitor the Internet sites I visit.
- **If I see something that I am unhappy with, or I receive messages I do not like, I will tell a teacher immediately.**
- Outside of school, any comments posted on Internet forums or social networking sites pertaining to the school should be respectful to the children, staff and reputation of the school.

Using e-mail:

- I will only email people I know or that the teacher has approved.
- The email messages that I send will be polite, sensible and linked to my learning.
- When sending email, I will not send my photo, home address, school address or telephone number to anyone, and I will never arrange to meet anyone.
- I will ask permission before opening an email or an email attachment sent by someone I do not know.

Pupil / Parent agreement:

I have read and understood the Rules for Responsible Internet Use. I will use the computer system and the Internet in a responsible way and will obey these rules at all times.

Pupil signature____ Date: ________________________

Parent signature ____ Date: ________________________