TOWNVILLE ACADEMY
Head teacher: Caroline Burden

Aspire - Collaborate - Explore

'Together we learn – United we achieve'

E-SAFETY POLICY

Our vision

At Townville Academy we aspire to offer the best possible early education for our children in a happy, safe, inclusive environment. We build firm foundations through a welcoming, holistic community approach placing the individual needs of the child at the heart. With high expectations and aspirations for every child we seek to ensure all children develop the skills and attributes they need to thrive and succeed both now and in the future.

Approved by:		***Date:*** *September 2024*
Last reviewed on:	*September 2024*	
Next review due by:	*September 2025*	

At Townville Academy we understand the responsibility we have to educate our pupils on e-safety issues; teaching them appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Townville Academy has a whole school approach to the safe use of ICT and creating this safe learning environment includes three main elements:

- *an effective range of technological tools*
- *policies and procedures, with clear roles and responsibilities*
- *a comprehensive e-safety programme for pupils, staff and parents.*

This policy is to be read in conjunction with all other policies particularly: Behaviour Policy, Safeguarding Policy and Child Protection Policy, Code of Conduct policy, Photography and Video Policy, and Equal Opportunities Policy.

We recognise that:

- *The internet is an essential element in 21st century life for education.*
- *The school has a duty to provide students with quality Internet access as part of their learning experience.*
- *Internet use is a necessary tool in school for staff and parents. The school is committed to the safeguarding and well-being of pupils.*

E-safety Co-ordinator: *Mrs C Burden (Headteacher & DSL)*
Deputy e-safety co-ordinator *Mrs J Cooper (DSL)*

E-SAFETY POLICY

1. *Responsibilities*

At Townville Academy we recognise that online safety is everyone's responsibility. Both our E-safety co-ordinators have received CEOP (Child Exploitation and Online Protection) training. Any concerns you have with regards E-safety should be brought to their attention.

Responsibility of e-safety Co-ordinator

- *Promote awareness and commitment to e-Safety throughout the school.*
- *Be the first point of contact in school on all e-Safety matters.*
- *Create and maintain e-Safety policies and procedures.*
- *Develop an understanding of current e-Safety issues.*
- *Ensure e-Safety is promoted to parents and carers.*
- *Ensure e-Safety is embedded across the curriculum.*
- *Ensure staff receive the appropriate level of training in e-Safety issues.*
- *Liaise with the Local Authority/Multi-Academy Trust on e-Safety matters.*
- *To be abreast of current issues and guidance, particularly with regards new technologies or trends.*
- *Working in partnership with the schools DSL team and ICT provider (Primary ICT) to*
    - *Ensure Filtering and Monitoring effectively limits students' exposure to risk.*
    - *Meet the appropriate digital and technology standards for schools.*

Responsibility of Teachers and Support Staff

- *Read and promote e-Safety policy and procedures.*
- *Supervise pupils carefully when engaging in internet activities.*
- *Be aware of what to do if a e-Safety incident occurs*
- *Maintain a professional level of conduct in their personal use of technology at all times.*
- *All staff should be familiar with the school's policy including:*
    - *safe use of e-mail*
    - *safe use of the Internet*
    - *safe use of the school network, equipment and data*
    - *safe use of digital images and digital technologies, such as mobile phones and digital cameras*
    - *publication of pupil information/photographs on the school website*
    - *procedures in the event of misuse of technology by any member of the school community (see appendices)*
    - *safe use of social media sites, including the schools Twitter account.*

Staff are reminded/updated about e-safety regularly and new staff receive information on the school's acceptable use policy as part of their induction. Supply Teachers must sign an acceptable use of ICT agreement before using technology equipment in school (see appendix 1 for staff acceptable use agreement).

Responsibility of Pupils

- *Adhere to school e-Safety policy.*
- *Understand what action you should take if you feel worried, uncomfortable, vulnerable or at risk whilst using technology.*

Responsibility of Parents

- *Help and support the school in promoting e-Safety.*
- *Take responsibility for learning about the benefits and risks of using the Internet and other technologies that your children use in school and at home.*
- *Encourage your children to behave safely and responsibly when using technology.*

Responsibility of Governing Body

- *Read, understand and help promote school e-Safety policy.*

- *Develop an overview of the benefits and risks of the internet used by pupils.*
- *Develop an overview of how the school ICT infrastructure provides safe access to the internet.*

2. Teaching and Learning

*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 material; for example, pornography, fake news, racism, misogyny, self-harm, suicide, anti semitism or radical and extremist views.*
- ***Contact:** being subjected to harmful online interaction with other users; for example, Child on Child pressure, commercial advertising as well as adults posing as children or young adults with the intention to groom and exploit them for financial, criminal, sexual or other purposes.*
- ***Conduct**: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (consensual and non-consensual sharing of nudes and semi nudes and 'or pornography, or online bullying and*
- ***Commerce**. Risks such as online gambling, inappropriate advertising, phishing or other financial scams.*

Students will be educated in online safety, and regularly reminded, as an ongoing part of our curriculum.

We believe that the key to developing a safe and responsible behaviour online lies in effective education. We know that the internet is embedded in our pupils' lives, and we believe we have a duty to help prepare our pupils to safely benefit from opportunities the internet brings. Computing and online resources are increasingly used across the curriculum. We believe it is essential for e-safety guidance to be given to the pupils on a regular and meaningful basis. We continually look for new ways to promote e-safety.

- *The school internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.*
- *Pupils will be taught, at an age-related level, what Internet use is acceptable and what is not and given clear objectives for Internet use.*
- *Pupils will be educated in the effective use of the Internet in research.*
- *Educating pupils on the dangers of technologies that may be encountered outside school is done informally, when opportunities arise and as part of the curriculum.*
- *Pupils are aware of the impact of online bullying through PSHE and know how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies.*

3. Managing Internet Access

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education as well as a potential risk to young people. Students will have supervised access to Internet resources through the school's fixed and mobile internet technology.

Staff will preview any recommended sites before use.

Raw image searches are discouraged when working with pupils.

If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise any further research.

Our internet access is controlled and filtered by Primary ICT.

Staff and pupils are aware that school-based email and internet activity can be monitored and explored further if required.

E-SAFETY POLICY

If staff or pupils discover an unsuitable site, the screen must be switched off/closed and the incident reported immediately to the e-safety co-ordinator.

It is the responsibility of the school, by delegation to the network manager, to ensure that anti-virus protection is installed and kept up-to-date on all school machines.

Any changes to filtering and monitoring must be authorised by a member of the senior leadership team in conjunction with the schools ICT provider.

As instructed by the school, Primary ICT will review and report upon the schools filtering and monitoring systems at least annually.

Information system security

- *The school is responsible for ensuring that, where reasonably possible access to the ICT systems is safe and secure as reasonably possible.*
- *Servers and other key hardware or infrastructure will be located securely with only appropriate staff permitted access*
- *Virus protection is installed on all appropriate hardware and will be kept up to date.*

E-Mail

- *Pupils may only use approved email accounts on the school system.*
- *Pupils must immediately tell a teacher is they receive an offensive email.*
- *Pupils must not reveal any personal details about themselves or others in email communications.*

School Website

- *The school website will not include the personal details, including individual email addresses, or full names of staff or pupils except where this is required for safeguarding purposes.*
- *A generic contact e-mail address will be used for all enquiries received through the website.*
- *All content included on the website will be approved by the Head teacher or E- Safety coordinator before publication.*

Publishing pupil's images and work

- *Parental permission will be gained to include any photographs of their child online in social media are via email.*
- *Pupils full names will not be used anywhere on the school website or Blogs, particularly in association with photographs*

Social networking and personal publishing

- *The school will block/filter access to social networking sites.*
- *Pupils will be advised never to give out personal details of any kind which may identify them or their location.*
- *Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for infant aged pupil.*

Managing Filtering

- *The school works in partnerships with the LA, Accomplish MAT, Primary ICT, DfE and the Internet Service provider to ensure systems to protect children are reviewed and improved*
- *If staff or pupils discover an unsuitable site, it must be reported to the e-safety co-ordinator and DSL lead who will be responsible for acting upon reports or concerns raised.*
- *As instructed by the school, Primary ICT will review and report upon the schools filtering and monitoring*

systems to the senior DSL and E-safety co-ordinator at least annually.

Protecting personal data

- *Personal data will be recorded, processed and transferred and made available according to the Data Protection Act 1998.*
- *Staff will ensure they properly log-off from a computer terminal after accessing personal data.*

4. Policy Decisions

Authorising Internet Access

- *Access to the internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.*

Assessing risks

- *The school will take all reasonable precautions to ensure that users access only appropriate material. However, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor the Trust can accept liability for the material accessed, or any consequence of Internet access.*
- *The school will audit ICT provision to establish if the e-Safety policy is adequate and that its implementation is effective.*

Handling E-Safety complaints

- *Complaints of Internet misuse will be dealt with by the Head teacher, or in their absence, a senior member of staff.*
- *Any complaint about staff misuse must be referred to the Head teacher/Senior DSL.*
- *Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.*

5. Communication

- *E-Safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year.*
- *Pupils will be informed that network and Internet use will be monitored.*
- *Staff will be given the e-Safety Policy.*
- *Parents' attention will be drawn to the school e-safety policy on the school website.*

6. E-safety Complaints/Incidents

As a school we take all precautions to ensure e-safety at all times. However, due to the international scale and linked nature of internet content, the availability of mobile technologies and the speed of change, it may mean that unsuitable material may briefly appear on a computer or mobile device. The school cannot accept liability for material accessed or any consequences of this. Complaints should be made to the Head teacher. Incidents should be logged and the flowchart for managing an e-safety incident is to be followed. It is important that the school work in partnership with pupils and parents to educate them about Cyber bullying and children, staff and families need to know what to do if they or anyone they know are a victim of Cyber bullying. All bullying incidents should be recorded and investigated via the incident log form.

Appendices

1. *Pupil Acceptable use agreement*
2. *Parent Form: Internet use*

Appendix 1

Townville Academy

Pupil Acceptable Use of ICT Agreement/E-Safety Rules

- ✓ I will only use ICT in school for school purposes.
- ✓ I will check with a grown up before using the internet.
- ✓ I will check with a grown up if something I see makes me feel worried.
- ✓ If I get stuck or lost on the internet I will ask for help.
- ✓ I will only write polite and friendly messages to people I know.
- ✓ I will keep my personal information, my name, address, my school, my pictures 'Top Secret' and not share it on an app or website.
- ✓ I will not bring mobile phones or tablets to school.
- ✓ I will only use my class e-mail address or my own school e-mail address when e-mailing.
- ✓ I will only open e-mail attachments from people I know, or who my teacher has approved.
- ✓ I will only open/delete my own files.
- ✓ I will not bring software, CDs or ICT equipment into school without permission.
- ✓ I will only use the Internet after being given permission from a teacher.
- ✓ I will not deliberately look for, save or send anything that could be upsetting or not allowed at school. If I accidentally find anything like this, I will close the screen and tell a teacher immediately.
- ✓ I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- ✓ I know that the school may check my use of ICT and monitor the Internet sites I have visited, and that my parent/carer will be contacted if a member of school staff is concerned about my eSafety.

Appendix 2

Dear Parents/Carers,

ICT, including the internet, e-mail and mobile technologies, has become an important part of learning in schools. We expect all children to be safe and responsible when using any ICT.

Please read and discuss with your child the E-Safety rules overleaf and return this sheet signed by both you and your child. If you have any concerns or would like some explanation, please contact your child's class teacher.

This Acceptable Use of ICT Agreement is a summary of our E-Safety Policy which is available in full on our website or as a hard copy in our Office/Reception.

We also ask that as a parent you agree to use and engage with our social media platforms, Twitter, Facebook and e-mail in a respectful manner. Social media platforms should not be used as a sounding board for any complaints. These should be directed straight to the head teacher via headteacher@townville.wakefield.sch.uk and will be responded to within 2 working days. Any parent malicious or derogatory posts which may bring the reputation of the school or its staff into question will be blocked from the use of our sites and maybe reported more widely.

Yours sincerely,

Caroline Burden
Headteacher

Pupil Name: *Class:*

I have read, understood and agreed with the Rules for Acceptable use of ICT.

Signed …….. (child)

Parent's/Carer's Consent for Internet Access

I have read and understood the school rules for Acceptable Use of ICT and give permission for my son / daughter to access the Internet in school. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the Internet.

I have read, understood and agree with the acceptable parental use of social media in relation to Townville Infants' and staff and agree to abide by these.

Signed…….. (parent/carer) *Date……*

Appendix 3

Staff, Governor and Visitor
Acceptable Use Agreement / Code of Conduct

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and *adhere at all times to its contents.*

- *I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Local Governing Board.*
- *I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.*
- *I will ensure that all electronic communications with pupils and staff are compatible with my professional role.*
- *I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.*
- *I will not use my personal internet enabled devices within the classroom or whilst working with children. (This includes but is not limited to mobile phones, smart watches etc)*
- *Personal communications are restricted to staff break times and are never conducted whilst a child/children are present.*
- *I will only use the approved, secure email system(s) for any school business.*
- *I will ensure that personal data (such as data held on Arbor/Aspire/CPOMs/Tapestry etc) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Local Governing Board.*
- *I will not use or install any hardware (including USB sticks) or software without permission from the e-safety co-ordinators.*
- *I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.*
- *Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Head teacher.*
- *I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request by the Head teacher.*
- *I will respect copyright and intellectual property rights.*
- *I will ensure that my online activity, both in school and outside school, will not bring my professional role or the reputation of the school into disrepute.*
- *I will support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.*
- *I will ensure that only children whose parents have given permission for them to use the Internet and ICT are enabled to do so at school.*

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school

Signature …… Date ……

Full Name …….... (printed)

Job title: …….

Appendix 4

Townville Academy
E-Safety Incident Log

Details of ALL e-safety incidents to be recorded in the Incident Log by the e-safety co-ordinator.
This incident log will be monitored termly by the e-safety co-ordinator and Head teacher.

Date & time	Name of pupil or staff member	Male or Female	Room and computer/device number	Details of incident (including evidence)	Actions and reasons