



Townlands C of E Primary Academy
Online Safety Policy

Approved by: Rachael Johnson (Chair of Governors)

Date: April 2026

Next review due by: April 2029

1. Introduction

- 1.1 Townlands C of E Primary Academy recognises the Internet and other digital technologies provide a vast opportunity for children and young people to learn. The Internet and digital technologies allow all those involved in the education of children and young people to promote creativity, stimulate awareness and enhance learning.
- 1.2 As part of our commitment to teaching and learning and achievement we at Townlands want to ensure that the Internet and other digital technologies are used to:
- Raise educational standards and promote pupil achievement.
 - Develop the curriculum and make learning exciting and purposeful.
 - Enable pupils to gain access to a wide span of knowledge in a way that ensures their safety and security.
 - Enhance and enrich their lives and understanding.
- 1.3 As part of this policy Townlands, holds steadfastly to the ethos that there should be an equitable learning experience for all pupils using ICT technology. We recognise that ICT can allow pupils with a disability increased access to the curriculum and other aspects related to learning.
- 1.4 Townlands is committed to ensuring that all its pupils will be able to use existing, as well as up and coming technologies safely. We are also committed to ensuring that all those who work with children and young people, as well as their parents, are educated as to the risks that exist so that they can take an active part in safeguarding children.
- 1.5 The nominated senior person for the implementation of the School's Online Safety policy is the Headteacher and all DSLs.

2. Scope of Policy

2.1 The policy applies to:

- all pupils
- all teaching and support staff (including peripatetic), school governors and volunteers
- all aspects of the School's facilities where they are used by voluntary, statutory or community organisations

2.2 Townlands will ensure that the following elements are in place as part of its safeguarding responsibilities to pupils:

- a list of authorised persons who have various responsibilities for Online safety
- a range of policies including acceptable use policies that are frequently reviewed and updated
- information to parents that highlights safe practice for children and young people when using the Internet and other digital technologies
- adequate training for staff and volunteers
- adequate supervision of pupils when using the Internet and digital technologies
- education that is aimed at ensuring safe use of Internet and digital technologies
- a reporting procedure for abuse and misuse.

3. Infrastructure and Technology

3.1 Partnership working

- 3.1.1 Townlands recognises that as part of its safeguarding responsibilities there is a need to work in partnership with our Internet Service Provider (ISP). As part of our commitment to partnership working, we fully support and will continue to work with our ISP to ensure that pupil and staff usage of the Internet and digital technologies is safe.
- 3.1.2 Townlands will, as part of its wider safeguarding responsibilities, seek to ensure that voluntary, statutory and community organisations take an approach to their activities that see the welfare of the child as paramount. To this end, we expect any organisation using the school's ICT or digital technologies to have appropriate policies and procedures that are aimed at safeguarding children and young people and reporting concerns.

4. Policies and Procedures

We at Townlands understand that effective policies and procedures are the backbone to developing a whole-school approach to online safety. The policies that exist within Townlands are aimed at providing a balance between exploring the educational potential of new technologies safeguarding pupils.

4.1 Use of Internet facilities, mobile and digital technologies

- 4.1.1 Townlands will seek to ensure that Internet, mobile and digital technologies are used effectively for their intended educational purpose, without infringing legal requirements or creating unnecessary risk.
- 4.1.2 Townlands expects all staff and pupils to use the Internet, mobile and digital technologies responsibly and strictly according to the conditions below:¹ These expectations are also applicable to any voluntary, statutory and community organisations that makes use of the school's ICT facilities and digital technologies.

Users shall not:

Visit Internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

- Indecent images of children
- Promoting discrimination of any kind
- Promoting racial or religious hatred
- Promoting illegal acts
- Any other information which may be offensive to peers or colleagues e.g. abusive images; promotion of violence; gambling; criminally racist or religious hatred material

- 4.1.3 Incidents which appear to involve deliberate access to websites, newsgroups and online groups that contain the following material will be reported to the Police:

¹ For the purposes of this document, Internet usage means any connection to the Internet via web browsing, external email, news groups or messaging services, mobile technologies e.g. mobile phone, including Bluetooth applications, PDA's etc.

- Images of child abuse (images of children whether they are digital or cartoons, apparently under 16 years old, involved in sexual activity or posed to be sexually provocative)
- Adult material that potentially breaches the Obscene Publications Act in the UK
- Criminally racist or anti-religious material
- Violence and bomb making
- Illegal taking or promotion of drugs
- Software piracy
- Other criminal activity

4.1.4 In addition, users may not:

- Use the ISP's facilities for running a private business
- Enter into any personal transaction that involves our ISP
- Visit sites that might be defamatory or incur liability on the part of our ISP
- Upload, download, or otherwise transmit (make, produce or distribute) commercial software or any copyrighted materials belonging to third parties outside of our ISP, or to our ISP itself
- Reveal or publicise confidential or proprietary information, which includes but is not limited to:
 - financial information, personal information, databases and the information contained therein, computer/network access codes, and business relationships
- Intentionally interfere with the normal operation of the Internet connection, including the propagation of computer viruses and sustained high volume network traffic (sending or receiving of large files or sending and receiving of large numbers of small files or any activity that causes network congestion) that substantially hinders others in their use of the Internet
- Use the Internet for soliciting, representing personal opinions or revealing confidential information or in any other way that could reasonably be considered inappropriate
- Transmit unsolicited commercial or advertising material either to other user organisations or to organisations connected to other networks, save where the material is embedded within, or is otherwise part of, a service to which the member of the user organisation has chosen to subscribe
- Assist with unauthorised access to facilities or services accessible via the school ISP
- Undertake activities with any of the following characteristics:
 - wasting staff effort or networked resources, including time on end systems accessible via our Internet Service Provider (ISP) network and the effort of staff involved in support of those systems
 - corrupting or destroying other users' data
 - violating the privacy of other users
 - disrupting the work of other users
 - using our ISP network in a way that denies service to other users (for example, deliberate or reckless overloading of access links or of switching equipment)
 - continuing to use an item of networking software or hardware after our ISP has requested that use cease because it is causing disruption to the correct functioning of our ISP
 - Other misuse of our ISP network, such as introduction of viruses
 - Use any mobile or digital technologies 3G or mobile Internet services in any way to intimidate, threaten or cause harm to others. Moreover, mobile technologies should

not be used to access inappropriate materials or encourage activities that are dangerous or illegal

- 4.1.5 Where our ISP become aware of an illegal act or an attempted illegal act, they will have to comply with the law as it applies and will take action directed by the police if a Regulation of Investigatory Powers Act (RIPA) Notice is issued.

4.2 Reporting Abuse

- 4.2.1 There will be occasions when either a pupil or an adult within the school receives an abusive email or accidentally accesses a website that contains abusive material. When such a situation occurs, the expectation of the school is that the pupil or adult should report the incident **immediately** to the Headteacher.
- 4.2.2 The School also recognises that there will be occasions where pupils will be the victims of inappropriate behaviour that could lead to possible or actual significant harm. The response of the School will be to take the reporting of such incidents seriously and where judged necessary, the Designated Safeguarding Lead for Child Protection within the School will refer details of an incident to the lead agencies involved in safeguarding children, namely Children's Social Care and the Police.

The School, as part of its safeguarding duty and responsibilities will assist and provide information and advice in support of child protection enquiries and criminal investigations.

5. Education and Training

- 5.1 Townlands recognises that the Internet and other digital technologies can transform learning; help to improve outcomes for children and young people; promote creativity; all of which add up to a more exciting and challenging classroom experience.
- 5.2 As part of achieving this, we want to create within Townlands an accessible system, with information and services online, which support personalised learning and choice. However, we realise that it will be necessary for our pupils to have the skills of critical awareness, digital literacy and good online citizenship to enable them to use the Internet and other digital technologies safely.
- 5.3 To this end, Townlands will: -
- Enable all pupils to exercise the skills of critical awareness, digital literacy and good online citizenship as part of the school curriculum
 - Educate school staff so that they are equipped to support pupils in gaining positive experiences when online and can help pupils develop strategies if they encounter a problem
 - Support parents in gaining an appreciation of Internet safety for their children and provide them with relevant information on the policies and procedures that govern the use of Internet and other digital technologies within the school

6. Standards and Inspection

Townlands recognises the need to have regular inspections of policies and procedures in order to ensure that its practices are effective and that the risks to pupils are minimised.

6.1 Filtering & Monitoring

The DfE guidance (for England) on filtering and monitoring in “Keeping Children Safe in Education” states:

“It is essential that governing bodies and proprietors ensure that appropriate filtering and monitoring systems are in place ...governing bodies and proprietors should be doing all that they reasonably can to limit children’s exposure to the ... risks from the school’s or college’s IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filtering and monitoring systems in place and regularly review their effectiveness. They should ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified...

The appropriateness of any filtering and monitoring systems are a matter for individual schools and colleges and will be informed in part, by the risk assessment required by the Prevent Duty. To support schools and colleges to meet this duty, the Department for Education has published filtering and monitoring standards...”

The school filtering and monitoring provision is agreed by senior leaders, governors and the IT Service Provider and is regularly reviewed (at least annually) and updated in response to changes in technology and patterns of online safety incidents/behaviours.

Townlands provides Internet filtering, designed to remove controversial, offensive or illegal content. However, it is impossible to guarantee that all controversial material is filtered. The school utilises a Sophos XG firewall provided and supported by the ISP that meets all the requirements set out by the DfE to apply the required filtering policies to ensure the Internet is safe and secure for all members of the school community. Weekly usage reports are provided to ensure filtering is working correctly and any areas of concern. Our school approach to online safety, including appropriate filtering and monitoring on school devices and school networks is reflected in this Child Protection Policy including awareness of the ease of access to mobile phone networks. (See KCSiE). If a member of staff discovers any websites containing inappropriate or offensive content, these need to be reported to technical support so that they can be filtered.

The DSL will have lead responsibility for safeguarding and online safety and the IT service provider will have technical responsibility.

- Checks on the filtering and monitoring system are carried out by the IT Service Provider with the involvement of senior leaders, the Designated Safeguarding Lead and a governor, in particular when a safeguarding risk is identified, there is a change in working practice, e.g. remote access or Bring your Own Device (BYOD) or new technology is introduced e.g. Wave 9 filtering and SENSO monitoring.

Filtering

- the school manages access to content across its systems for all users and on all devices using the schools internet provision. The filtering provided meets the standards defined in the DfE Filtering standards for schools and colleges and the guidance provided in the UK Safer Internet Centre [Appropriate filtering.](#)

- Illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content (CTIRU), produced on behalf of the Home Office and blocking access to illegal content including child sexual abuse material (CSAM).
- Content lists are regularly updated.
- there are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective
- there is a clear process in place to deal with, and log, requests/approvals for filtering changes
- Filtering logs are regularly reviewed and alert the Designated Safeguarding Leads to breaches of the filtering policy, which are then acted upon.
- the school has a mobile phone policy.
- If necessary, the school will seek advice from, and report issues to the filtering provider.

Monitoring

The school has monitoring systems in place to protect the school, systems and users:

- The school monitors all network use across all its devices and services.
- Monitoring reports are picked up at pace, acted on and outcomes are recorded by the Designated Safeguarding Leads, all users are aware that the network (and devices) are monitored.
- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention.
- Management of serious safeguarding alerts is consistent with safeguarding policy and practice.

The school follows the UK Safer Internet Centre [Appropriate Monitoring](#) guidance and protects users and school systems through the use of the appropriate blend of strategies informed by the school's risk assessment. These may include:

- physical monitoring (adult supervision in the classroom)
- internet use is logged, regularly monitored and reviewed
- filtering logs are regularly analysed and breaches are reported to senior leaders
- pro-active alerts inform the school of breaches to the filtering policy, allowing effective intervention
- use of a third-party assisted monitoring service which allows DSLs to monitor internet browsing

Technical Security

The school technical systems will be managed in ways that ensure that the school meets recommended technical requirements

- responsibility for technical security resides with SLT who may delegate activities to identified roles
- all users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the IT service provider and will be reviewed, at least annually, by SLT

- policies and procedures are implemented
- the security of their username and password and must not allow other users to access the systems using their log on details
- all users have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details
- all school networks and system will be protected by secure passwords. Passwords must not be shared with anyone
- the administrator passwords for school systems are stored securely with our IT service provider
- there will be regular reviews and audits of the safety and security of school technical systems
- servers, wireless systems and cabling are securely located and physical access restricted
- appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems and devices from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date endpoint software
- there are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud
- an appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed
- use of school devices out of school is regulated by an acceptable use statement that a user consents to when the device is allocated to them
- personal use of any device on the school network is regulated by acceptable use statements that a user consents to when using the network
- staff members are not permitted to install software on a school-owned devices without the consent of the SLT/IT service provider
- removable media is not permitted unless approved by the SLT/IT service provider
- systems are in place to control and protect personal data and data is encrypted at rest and in transit
- guest users are provided with appropriate access to school systems based on an identified risk profile
- Monitoring the safe use of the Internet and other digital technologies goes beyond the personal use of the Internet and electronic mail a pupil or member of staff may have. Townlands recognises that in order to develop an effective whole school Online safety approach there is a need to monitor patterns and trends of use inside school and outside school (Education and Inspections Act 2006, Section 89(5))
- 6.1.2 With regard to monitoring trends, within the school and individual use by school staff and pupils, Townlands will audit the use of the Internet and electronic mail in order to ensure compliance with this policy. The monitoring practices of the school are influenced by a range of national and Local guidance documents and will include the monitoring of content and resources.
- 6.1.3 Another aspect of monitoring, which our school will employ, is the use of mobile technologies by pupils, particularly where these technologies may be used to cause harm to others, e.g. bullying (see anti-bullying policy for further information). We will also ensure that

school staff understand the need to monitor our pupils, and where necessary, support individual pupils where they have been deliberately or inadvertently been subject to harm.

6.2 Sanctions

6.2.1 Townlands has been careful to develop in conjunction with its partners, policies and procedures to support the innocent in the event of a policy breach and enable the School to manage such situations in, and with, confidence.

6.2.2 Where there is inappropriate or illegal use of the Internet and digital technologies, the following sanctions will be applied:

- Child / Young Person:
 - The child/young person will be disciplined according to the Behaviour Policy of the school, which could ultimately include the use of Internet and email being withdrawn
 - Serious breaches may lead to the incident being reported to the Police or other regulatory bodies, for instance, illegal Internet use or child protection concerns.
- Adult (Staff and Volunteers)
 - The adult may be subject to the disciplinary process, if it is deemed he/she has breached the policy
 - Serious breaches may lead to the incident being reported to the Police or other regulatory bodies, for instance, illegal Internet use or child protection concerns.

7. Working in Partnership with Parents and Carers

7.1 Townlands is committed to working in partnership with parents and carers and understands the key role they play in the Internet safety of their children, through promoting Internet safety at home and elsewhere.

7.2 We at Townlands also appreciate that there may be some parents who are concerned about the use of the Internet, email and other digital technologies in school. In such circumstances school staff will meet with parents and carers to discuss their concerns and agree upon a series of alternatives that will allow their child to fully access the curriculum, whilst remaining safe.

8. Links to other policies

- The Teaching Standards
- Disciplinary Policy
- Safeguarding Policy
- Keeping Children Safe in Education (KCSIE)
- Guidance for Safer Working Practice for those working with children in Education settings
- Behaviour Policy
- Data Protection Policy
- Information Security Policy
- Mobile Phone Policy
- Whistle blowing Policy