Title	**Online Safety Policy - TTA**
Policy Owner	**Safeguarding Lead/School Business Manager**
Effective Date	**September 2023**
Last Revised	**August 2023**
Next Review Date	**August 2025**

1. Schedule for development / monitoring / review

This online safety policy was approved by the Board of Directors/Governing Body/Governors Sub Committee on:	21st November 2023
The implementation of this online safety policy will be monitored by the:	School Business Manager
Monitoring will take place at regular intervals:	Once a year
The Governing Body/Governors Sub Committee will receive a report on the implementation of the online safety policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	Once a year
The online safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	Autumn 2024
Should serious online safety incidents take place, the following external persons/agencies should be informed as necessary:	LA Safeguarding Officer, Academy Group Officials, LADO, Police

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)/filtering
- Internal monitoring data for network activity
- Surveys/questionnaires of
    - students/pupils
    - parents/carers
    - staff

2. Scope of the Policy

This policy applies to all members of the Totteridge Academy community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of The Totteridge Academy digital technology systems, both in and out of the Totteridge Academy.

The Education and Inspections Act 2006 empowers Headteachers/Principals to such extent as is reasonable, to regulate the behaviour of students/pupils when they are off the Totteridge Academy site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other online safety incidents covered by this policy, which may take place outside of the Totteridge Academy but is linked to membership of the Totteridge Academy. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The Totteridge Academy will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

3. Aims

The Totteridge Academy aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology.
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

4. Legislation and guidance

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

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

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 considers the National Curriculum computing programmes of study.

5. Roles and responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school/academy:

5.1 The Local Governing Body (LGB)

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

A member of the senior leadership team and a governor, to be responsible for ensuring filtering and monitoring standards are met.

The LGB will co-ordinate regular meetings with appropriate staff to discuss online safety, monitor online safety logs as provided by the designated safeguarding lead (DSL) and ensure the effectiveness of filtering and monitoring is regularly reviewed (at least annually).

All governors will:

- Ensure that 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

The governor who oversees online safety is Bronwen Tumani and is responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy.

This will be carried out by the LGB receiving regular information about online safety incidents and monitoring reports. A member of the LGB has taken on the role of Online Safety Governor and this role includes:

- regular meetings with the Online Safety Co-ordinator/officer
- attendance at Online Safety Group meetings
- regular monitoring of online safety incident logs
- regular monitoring of filtering/change control logs
- reporting to relevant LGB meeting}

5.2 The Principal and the Senior Leadership Team

- The Principal is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.
- The Principal has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the Online Safety Lead.
- The Principal and Senior Vice Principal should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff and should refer to safeguarding policy.
- The Principal and Senior Leaders are responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Principal and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a

safety net and also support to those colleagues who take on important monitoring roles. They will document decisions on what is blocked or allowed and why.

- Systems: Impero, LGFL Firewall, Office 365 Filtering Policy.
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Lead and review the effectiveness of the provision.5.3 The designated safeguarding lead

Details of the school's DSL/DDSLs are set out in Annex C of Keeping Children Safe in Education (DfE).

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

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged 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
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board
- Overseeing checks to filtering and monitoring systems

This list is not intended to be exhaustive.

5.4 The IT Network Manager

The IT Network Manager is responsible for:

- Putting in place and maintaining appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils 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 weekly 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 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.

5.5 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 and ensuring that pupils follow the school's terms on acceptable use.
- Working with the DSL to ensure that any online safety incidents are logged 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.

5.6 Parents

Parents 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.

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? - UK Safer Internet Centre
- Hot topics - Childnet International
- Parent factsheet - Childnet International
- Healthy relationships – Disrespect Nobody

5.7 Visitors and members of the community

Visitors and members of the community who access The Totteridge Academy systems or programmes or use the school's ICT systems or internet as part of the wider Totteridge Academy provision will be made aware of this policy (when relevant) and will be expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use and sign a Community User AUA before being provided with access to The Totteridge Academy systems.

5.8 Pupils

- are responsible for using the Totteridge Academy digital technology systems in accordance with the student/pupil acceptable use agreement policy documentation.
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on online-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's/academy's online safety policy covers their actions out of school, if related to their membership of the school

6. Education and training

6.1 Educating Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety/digital literacy is therefore an essential part of the Totteridge Academy's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

In **Key Stage 3**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

*By the **end of secondary school**, pupils will know:*

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

All schools - adapt this to reflect your school's approach:

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

6.2 Educating Parents/Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an

essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The Totteridge Academy will therefore seek to provide information and awareness of internet safety, as well as reinforce the importance of children being safe online, to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site, Learning Platform
- Parents/carers evenings/sessions
- High profile events/campaigns e.g. Safer Internet Day
- Reference to the relevant web sites/publications

This policy will also be shared with parents.

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

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6.4 Educating and training staff/volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the {school/academy} online safety policy and acceptable use agreements.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- The Online Safety Lead (or other nominated person) will receive regular updates through attendance at external training events (e.g. from SWGfL/LA/other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This online safety policy and its updates will be presented to and discussed by staff in staff/team meetings/training sessions.
- The Online Safety Lead (or other nominated person) will provide advice/guidance/training to individuals as required.

6.5 Educating and training staff/volunteers

Members of the LGB should take part in online safety training/awareness sessions, with particular importance for those who are members of any group involved in technology/online safety/health and safety /safeguarding.

This may be offered in several ways:

- Attendance at training provided by the Local Authority/United Learning/National Governors Association/or other relevant organisation
- Participation in The Totteridge Academy's training/information sessions for staff or parents

7. Protecting children from online abuse

Taken from the NSPCC "Protecting children from online abuse"(23.12.2020)

Online abuse is any type of abuse that happens on the internet, facilitated through technology like computers, tablets, mobile phones and other internet-enabled devices (Department for Education, 2018; Department of Health, 2017; Scottish Government, 2014; Welsh Assembly Government, 2018).

It can happen anywhere online that allows digital communication, such as:

- social networks
- text messages and messaging apps
- email and private messaging
- online chats
- comments on live streaming sites
- voice chat in games.

Children and young people can be revictimised (experience further abuse) when abusive content is recorded, uploaded or shared by others online. This could happen if the original abuse happened online or offline. Children and young people may experience several types of abuse online:

- bullying/cyberbullying
- emotional abuse (this includes emotional blackmail, for example pressuring children and young people to comply with sexual requests via technology)
- sexting (pressure or coercion to create sexual images)
- sexual abuse
- sexual exploitation.

Children and young people can also be groomed online: perpetrators may use online platforms to build a trusting relationship with the child in order to abuse them. This abuse may happen online or the perpetrator may arrange to meet the child in person with the intention of abusing them.

7.1 Cyber-bullying
Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

7.2 Emotional Abuse
Emotional abuse is emotional maltreatment of a child, which has a severe and persistent negative effect on the child's emotional development (Department for Education, 20171; Department of Health, 20172; Scottish Government, 20143; Wales Safeguarding Procedures Project Board, 20194). It's also known as psychological abuse.

Most forms of abuse include an emotional element, but emotional abuse can also happen on its own. Children can be emotionally abused by anyone:

- parents or carers
- family members

- other adults
- other children

Online examples of emotional abuse can include (but are not limited to):

- verbal humiliation
- name-calling
- criticism
- restricting social interaction
- exploiting or corrupting
- encouraging a child to take part in criminal activities
- forcing a child to take part in activities that are not appropriate for their stage of development
- terrorising
- threatening violence
- bullying
- deliberately frightening a child
- deliberately putting a child in a dangerous situation

7.3 Consensual and non-consensual sharing of nudes and semi-nude images and or videos (also known as sexting or youth produced sexual imagery);

This is when people share a sexual message and/or a naked or semi-naked image, video or text message with another person. It's also known as nude image sharing.

Children and young people may consent to sending a nude image of themselves. They can also be forced or coerced into sharing images by their peers or adults online.

If a child or young person originally shares the image consensually, they have no control over how other people might use it.

If the image is shared around peer groups, it may lead to bullying and isolation. Perpetrators of abuse may circulate a nude image more widely and use this to blackmail a child and/or groom them for further sexual abuse.

It's a criminal offence to create or share explicit images of a child (anyone under the age of 18), even if the person doing it is a child. If reported to the police, they will make a record but may decide not to take any formal action against a young person.

7.4 Sexual abuse

Child sexual abuse (CSA) is when a child is forced or persuaded to take part in sexual activities. This may involve physical contact or non-contact activities and can happen online or offline (Department for Education, 2018; Department of Health, Social Services and Public Safety, 2017; Scottish Government, 2014; Wales Safeguarding Procedures Project Board, 2019). Children and young people may not always understand that they are being sexually abused.

Contact abuse involves activities where an abuser makes physical contact with a child. It includes:

- sexual touching of any part of the body, whether the child is wearing clothes or not
- forcing or encouraging a child to take part in sexual activity
- making a child take their clothes off or touch someone else's genitals
- rape or penetration by putting an object or body part inside a child's mouth, vagina or anus.

Non-contact abuse involves activities where there is no physical contact. It includes:

- flashing at a child
- encouraging or forcing a child to watch or hear sexual acts
- not taking proper measures to prevent a child being exposed to sexual activities by others
- making a child masturbate while others watch
- persuading a child to make, view or distribute child abuse images (such as performing sexual acts over the internet, sexting or showing pornography to a child)
- making, viewing or distributing child abuse images
- allowing someone else to make, view or distribute child abuse images
- meeting a child following grooming with the intent of abusing them (even if abuse did not take place)
- sexually exploiting a child for money, power or status (child sexual exploitation).

7.5 Child Sexual Exploitation

Child sexual exploitation (CSE) is a type of child sexual abuse. It occurs where an individual or group takes advantage of an imbalance of power to coerce, manipulate or deceive a child or young person under the age of 18 into sexual activity (Department for Education, 2017; NIdirect, 2018; Scottish Government, 2018; Wales Safeguarding Procedures Project Board, 2019).

Children and young people in sexually exploitative situations and relationships are persuaded or forced to perform sexual activities or have sexual activities performed on them in return for gifts, drugs, money or affection.

CSE can take place in person, online, or using a combination of both.

Perpetrators of CSE use a power imbalance to exploit children and young people. This may arise from a range of factors including:

- age
- gender
- sexual identity

- cognitive ability
- physical strength
- status
- access to economic or other resources (Department of Education, 2017).

Sexual exploitation is a hidden crime. Young people have often been groomed into trusting their abuser and may not understand that they're being abused. They may depend on their abuser and be too scared to tell anyone what's happening because they don't want to get them in trouble or risk losing them. They may be tricked into believing they're in a loving, consensual relationship.

When sexual exploitation happens online, young people may be persuaded or forced to:

- have sexual conversations by text or online
- send or post sexually explicit images of themselves
- take part in sexual activities via a webcam or smartphone (Hamilton-Giachritsis et al, 2017).

Abusers may threaten to send images, video or copies of conversations to the young person's friends and family unless they take part in further sexual activity. Images or videos may continue to be shared long after the sexual abuse has stopped.

7.6 Radicalisation

Information taken from: https://www.getsafeonline.org/social-networking/online-radicalisation/

Radicalisation by extremist groups or individuals can be perpetrated via several means: face-to-face by peers, in organised groups in the community and, increasingly, online. Their targets are individuals or groups of people who can be easily led towards terrorist ideologies because of their experiences, state of mind or sometimes their upbringing.

However extremists attempt to influence vulnerable people, the internet invariably plays some kind of role … being widely used both to create initial interest, and as reinforcement to other means of communication. As is the case with everything it is used for, the internet enables considerably larger numbers of people to be reached, in a wider geographic area, and with less effort by the perpetrators.

The power of social media is well-known, and it is this that is the main channel for such grooming – be it Facebook, Twitter or the multitude of other sites and apps. Other online channels include chatrooms, forums, instant messages and texts. All are also used by extremists for their day-to-day communication, as is the dark web.

Social media is also used for research by extremists, making it easy for them to identify those who may be vulnerable from what they reveal in their profiles, posts/tweets, photos and friend lists.

7.7 The school's response to online abuse

To help prevent online abuse 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 examples of online abuse 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 examples of online abuse. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on examples of online abuse its impact and ways to support pupils, as part of safeguarding training.

The school also sends information/leaflets on examples of online abuse to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of online abuse, 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 consider whether the incident should be reported to the police if it involves illegal material and will work with external services if it is deemed necessary to do so.

8. Mobile technologies (including BYOD/BYOT)

UL Policy: *https://hub.unitedlearning.org.uk/sites/policies/Technology Policies/Bring Your Own Device Policy (Temporary School Closures).docx*

Accessing United Learning Data using your own device policy:
https://hub.unitedlearning.org.uk/sites/policies/Technology%20Policies/Accessing%20United%20Learning%20Data%20Using%20your%20Own%20Device%20Policy.docx

9. Use of digital and video images

Link to United Learning Copyright Policy:
https://hub.unitedlearning.org.uk/sites/policies/Technology%20Policies/Copyright%20and%20PRS.docx

10. Data protection

When sharing information staff will ensure they comply with group data protection policies and keep records of disclosures as required by these policies.

11. Technical infrastructure/equipment, filtering and monitoring

If the Totteridge Academy has a managed ICT service provided by an outside contractor, it is the responsibility of the Totteridge Academy to ensure that the managed service provider carries out all the online safety measures

that would otherwise be the responsibility of the school/academy, as suggested below. It is also important that the managed service provider is fully aware of the Totteridge Academy's online safety policy/acceptable use agreements. The Totteridge Academy should also check their Local Authority/MAT /other relevant body policies on these technical issues.

The Totteridge Academy will be responsible for ensuring that the Totteridge Academy's infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- *The Totteridge Academy Technical systems will be managed in ways that ensure that The Totteridge Academy meets recommended technical requirements as set out in the Department for Education's "Meeting digital and technology standards in schools and colleges"*
- *There will be regular reviews* (at least annually or when: a safeguarding risk is identified, there is a change in working practice and/or new technology is introduced) and checks** of the safety and security of The Totteridge Academy technical systems). These will be recorded.*
- *Servers, wireless systems and cabling must be securely located and physical access restricted*
- *All users will have clearly defined access rights to The Totteridge Academy's technical systems and devices.*
- *All users (at KS2 and above) will be provided with a username and secure password by the IT Network Manager who will keep an up-to-date record of users and their usernames. Users are responsible for the security of their username and password. (Schools/academies may choose to use group or class logons and passwords for KS1 and below, but should consider whether this models good password practice and need to be aware of the associated risks – see appendix)*
- *The "master/administrator" passwords for the Totteridge Academy systems, used by the Network Manager must also be available to the Head/Principal or other nominated senior leader and kept in a secure place.*
- *(Sadek Amine – IT Network Manager) is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations (Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs)*
- *Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. (the Totteridge Academy will need to decide on the merits of external/internal provision of the filtering service – see appendix). There is a clear process in place to deal with requests for filtering changes (see appendix for more details)*
- *Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet. N.B. additional duties for schools/academies under the Counter Terrorism and Securities Act 2015 which requires schools/academies to ensure that children are safe from terrorist and extremist material on the internet. (see appendix for information on "appropriate filtering").*
- *The Totteridge Academy has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different ages/stages and different groups of users – staff/pupils/students etc)*
- *The Totteridge Academy technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement.*
- *An appropriate system is in place (to be described) for users to report any actual/potential technical incident/security breach to the relevant person, as agreed).*

- *Appropriate security measures are in place (schools/academies may wish to provide more detail) to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices, etc. 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 devices are protected by up-to-date virus software.*
- *An agreed policy is in place (to be described) for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems.*
- *An agreed policy is in place (to be described) regarding the extent of personal use that users (staff/students/pupils/community users) and their family members are allowed on school devices that may be used out of school.*
- *An agreed policy is in place (to be described) that allows staff to/forbids staff from downloading executable files and installing programmes on school devices.*
- *An agreed policy is in place (to be described) regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on school devices.* ***Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured****. (see School Personal Data Policy Template in the appendix for further detail)}*

12. How the school will respond to issues of misuse

It is hoped that all members of the Totteridge Academy community will be responsible users of digital technologies, who understand and follow The Totteridge Academy's policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority/Academy Group or national/local organisation (as relevant).
    - Police involvement and/or action
- **If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**

- incidents of 'grooming' behaviour
- the sending of obscene materials to a child
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- promotion of terrorism or extremism
- offences under the Computer Misuse Act
- other criminal conduct, activity or materials

- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all the above steps are taken as they will provide an evidence trail for the Totteridge Academuy and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

Specific pupil/staff misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on ICT acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the [staff disciplinary procedures/staff code of conduct]. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

13. References, further reading and useful links

GOV.UK (30.6.2020), 'Guidance: Education for a Connected World', Available at: https://www.gov.uk/government/publications/education-for-a-connected-world

Gov.uk - Meeting digital and technology standards in schools and colleges

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

NSPCC Learning 23.12.2020), 'Protecting children from online abuse', Available at: https://learning.nspcc.org.uk/child-abuse-and-neglect/online-abuse

SWGfL (2020), '{school/academy} Online Safety Policy Template', Available at: https://swgfl.org.uk/resources/online-safety-policy-templates/

The Key (23.12.2020), 'Online safety policy: models and examples', Available at: https://schoolleaders.thekeysupport.com/policy-expert/pastoral/online-safety-policy-model-examples/#section-0

United Learning (2021), 'Policies Portal', Available at: https://hub.unitedlearning.org.uk/sites/policies

*Any review will need to understand:

- the risk profile of your pupils, including their age range, pupils with special educational needs and disability (SEND), pupils with English as an additional language (EAL)
- what your filtering system currently blocks or allows and why
- any outside safeguarding influences, such as county lines
- any relevant safeguarding reports
- the digital resilience of your pupils
- teaching requirements, for example, your RHSE and PSHE curriculum
- the specific use of your chosen technologies, including Bring Your Own Device (BYOD)
- what related safeguarding or technology policies you have in place
- what checks are currently taking place and how resulting actions are handled

** Checks to your filtering provision need to be completed and recorded as part of your filtering and monitoring review process. How often the checks take place should be based on your context, the risks highlighted in your filtering and monitoring review, and any other risk assessments. Checks should be undertaken from both a safeguarding and IT perspective.

When checking filtering and monitoring systems you should make sure that the system setup has not changed or been deactivated. The checks should include a range of:

- school owned devices and services, including those used off site
- geographical areas across the site
- user groups, for example, teachers, pupils and guests

You should keep a log of your checks so they can be reviewed. You should record:

- when the checks took place
- who did the check
- what they tested or checked
- resulting actions