Tudor Grange Academies Trust

Tudor Grange Academy Worcester

Online Safety Policy and ICT Acceptable User Agreements

Document title	Tudor Grange Academy Worcester Safety Policy and ICT Acceptable User Agreements
Author/originator	C Waterhouse, R Mann, S Groutage, D Butler
Date of Approval/Review	16th July 2023
Approving Committee	Operations Committee
Version	2.0
Policy review date	Annual – July 2024

Date updated	Version	Change from last version
July 2020		
24.01.2022	1.2	
16.07.2023	2.0	Annual review. New Section 1 and subsequent renumbering. New section 3. Update para 4.2. Formatting and numbering changes to paragraphs 4.3, 4.4, 5.4 to 5.7, 6.5 to 6.10, section 8. New section 7 and subsequent renumbering Update to paragraph 9.1.1, 9.2.1. New paragraphs 9.3.3 and 9.3.4 Appendix 1 – addition of links to 'Childline/IWF Report Remove' tool and 'Report harmful content' Rewrite of Appendix 2 and 3 Acceptable use agreements Addition of paragraph 3.5.3 from KCSIE 2023

Contents

1 Scope....3

2 Rationale....3

3 Policy and Leadership....3

4 Risk and Harms....7

5 Curriculum context....9

6 Managing Information Systems....14

7 Breaches....18

8 Policy decisions....19

9 Awareness and Communication....21

Appendix 1: e-Safety Information, Advice and Support....23

Appendix 2: Staff (and Volunteer) Acceptable Use Policy Agreement....27

Appendix 3: Pupil Acceptable Use Policy Agreements....30

Acceptable Use Agreement for 6th Form Learners....30

Acceptable Use Agreement for Key Stage 3 & 4 Learners....33

Acceptable Use Agreement for Key Stage 2 Learners....36

Acceptable Use Agreement for Key Stage 1 Learners.....38

Acceptable Use Agreement for Foundation and entry level Key Stage 1 Learners.....40

Appendix 4: How to Report Abuse on Social Media....41

Appendix 5: Young People's Rights on Social Media....42

1 Scope

1.1 This Online Safety Policy outlines the commitment of Tudor Grange Academies Trust to safeguard members of our school communities online in accordance with statutory guidance and best practice.

1.2 This Online Safety Policy applies to all members of the school community (including staff, learners, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

1.3 Schools will deal with such incidents within this policy and associated behaviour and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that takes place out of school.

1.4 Associated Academy Policies:

- Safeguarding Policy
- Acceptable Use Agreements (see Appendices 2 and 3)
- Health and Safety Policy
- Data Protection Policy
- Consent for Using Pupils' Images
- Behaviour Policy

2 Rationale

2.1 Tudor Grange Academies Trust is committed to a policy of protecting the children and young people in our care, in line with the law. Today's children are growing up in an increasingly complex world, living their lives seamlessly on and offline. This presents many positive and exciting opportunities, but also challenges and risks. We want our schools to equip children with the knowledge needed to make the best use of the internet and technology in a safe, considered and respectful way, so they are able to reap the benefits of the online world. This advice brings together information that will help schools deliver online safety content within their curriculum and embed this within their wider whole school approach.

3 Policy and Leadership

3.1 To ensure the online safeguarding of members of our school community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals and groups within the school.

3.2 Principal and Senior Leaders

3.2.1 The Principal has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety may be delegated to the Online Safety Co-Ordinator.

3.2.2 The Principal and (at least) another member of the Senior Leadership Team 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.

3.2.3 The Principal/Senior Leaders are responsible for ensuring that the Online Safety Co-ordinator, technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.

3.2.4 The Principal/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.

3.2.5 The Principal/Senior Leaders will receive regular monitoring reports from the Online Safety Co-Ordinator.

3.3 Governance

3.3.1 The DfE guidance "Keeping Children Safe in Education" states:

> "Governing bodies and proprietors should ensure there are appropriate policies and procedures in place in order for appropriate action to be taken in a timely manner to safeguard and promote children's welfare …. this includes … online safety"

3.3.2 The Operations Committee are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This review will be carried out by the Operations Committee whose members will receive regular information about online safety incidents and monitoring reports.

3.4 Online Safety Co-Ordinator

3.4.1 The Online Safety Co-ordinator will co-ordinate online safety following the TGAT Online Safety Framework, with the aim of achieving National Online Safety Certified School status and 360 Safe Online Safety Mark. This includes:

- Achieving National Online Safety Certified School status by ensuring all staff login to https://nationalonlinesafety.com/ and ensure all staff complete Annual Certificate in Online Safety for Staff and Practitioners.
- Ensuring completion of the Annual Advanced Certificate in Online Safety for DSLs & Deputy DSLs.
- Co-ordinating parents to complete the Annual Certificate in Online Safety for Parents & Carers of Children.
- Completing all tasks in the 'Committed to Safety Online' and then 'Progression to Safety Online' sections of the TGAT Online Safety Framework.
- Ultimately achieving the 360 Online Safety Mark by completing all tasks in the 'Accredited Safer Online' section and being assessed by the 360 Safe Assessor.

3.5 Designated Safeguarding Lead (DSL)

3.5.1 The DfE guidance "Keeping Children Safe in Education" states:

- "The designated safeguarding lead should take lead responsibility for safeguarding and child protection (**including online safety**). This should be explicit in the role holder's job description." … Training should provide designated safeguarding leads with a good

understanding of their own role, … so they … are able to understand the unique risks associated with **online safety** and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online at school or college."

3.5.2 The Designated Safeguarding Lead should be trained in online safety issues and be aware of the potential for serious safeguarding issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate online contact with adults/strangers
- potential or actual incidents of grooming
- online bullying

3.5.3 The Designated Safeguarding Lead has lead responsibility for the understanding and the filtering and monitoring systems in place to protect pupils.

3.6 Curriculum Leads

3.6.1 Curriculum Leads will work with the Online Safety Lead to develop a planned and coordinated online safety education programme. This will be provided through:

- The ICT curriculum
- PHSE and SRE programmes
- A mapped cross-curricular programme
- assemblies and pastoral programmes
- through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

3.7 Teaching and Support Staff

3.7.1 School staff are responsible for ensuring that:

- they have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices
- they understand that online safety is a core part of safeguarding
- they have read, understood, and signed the staff acceptable use agreement (AUA)
- they immediately report any suspected misuse or problem to your line manager for investigation/action, in line with the school safeguarding procedures
- all digital communications with learners and parents/carers should be on a professional level *and only carried out using official school systems*
- online safety issues are embedded in all aspects of the curriculum and other activities
- ensure learners understand and follow the Online Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices

- in lessons where internet use is pre-planned learners should be guided to sites checked as suitable for their use *and that processes are in place for dealing with any unsuitable material that is found in internet searches*
- where lessons take place using live-streaming or video-conferencing, staff must have full regard to national safeguarding guidance and local safeguarding policies and should take note of the guidance contained in the SWGfL Safe Remote Learning Resource
- have a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.

3.8 **Network Manager/Technical Staff**

3.8.1 The Network Manager/Technical Staff is responsible for ensuring that:

- they are aware of and follow the school Online Safety Policy and Technical Security Policy to carry out their work effectively in line with school policy
- the school technical infrastructure is secure and is not open to misuse or malicious attack
- the school meets (as a minimum) the required online safety technical requirements as identified by the local authority/MAT or other relevant body
- there is clear, safe, and managed control of user access to networks and devices
- they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- the use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to (insert relevant person) for investigation and action
- the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person (see 'Technical Security Policy template' for good practice).
- monitoring software/systems are implemented and regularly updated as agreed in school policies

3.9 **Learners**

3.9.1 All learners are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement and Online Safety Policy (this should include personal devices where allowed).

3.9.2 All learners should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

3.9.3 All learners should know what to do if they or someone they know feels vulnerable when using online technology.

3.9.4 All learners should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

3.10 **Parents and carers**

3.10.1 Parents and carers play a crucial role in ensuring that their children understand the need to use the online services and devices in an appropriate way. The school will take every opportunity to help parents and carers understand these issues through:

- publishing the school Online Safety Policy on the school website
- providing them with a copy of the learners' acceptable use agreement (the school will need to decide if they wish parents/carers to acknowledge these by signature)
- publish information about appropriate use of social media relating to posts concerning the school
- seeking their permissions concerning digital images, cloud services etc (see parent/carer AUA in the appendix)
- parents'/carers' evenings, newsletters, website, social media and information about national/local online safety campaigns and literature.

3.10.2 Parents and carers will be encouraged to support the school in:

- reinforcing the online safety messages provided to learners in school
- the use of their children's personal devices in the school (where this is allowed)

3.11 **Community users**

3.11.1 Community users who access school systems/website/learning platform as part of school provision will be expected to sign a community user Acceptable Use Agreement before being provided with access to school systems.

3.11.2 The school encourages the engagement of agencies/members of the community who can provide valuable contributions to the online safety provision and actively seeks to share its knowledge and good practice with other schools and the community.

4 Risk and Harms

4.1 If we are to effectively safeguard our school communities, we must first understand where e-safety risks and potential harms lie. Unfortunately, the breadth of the issues classified within the term 'online safety' is considerable. Therefore, we have adopted the domains and definitions, as stated within key safeguarding guidance, (Keeping Children Safe in Education). These '4 Cs' are listed as follows:

4.1.1 Content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.

4.1.2 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.

4.1.3 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.

4.1.4 Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams. Pupils or staff at risk can be reported to the Anti-Phishing Working Group (https://apwg.org/)

4.2 It is noted that where concerns pertain to sexualised harms are reported, staff are aware of the DfE searching screening and confiscation at schools guidance and Sharing nudes and semi-nudes: advice for education settings working with children and young people. The key consideration is for staff not to view or forward illegal images of a child. The highlighted advice provides more details on what to do when viewing an image is unavoidable. In some cases, it may be more appropriate to confiscate any devices to preserve any evidence and hand them to the police for inspection.

4.3 Cybercrime

4.3.1 Keeping Children Safe in Education has been updated to reflect the advances and emergence of wider e-safety harms and now makes specific reference to this issue. This relates to criminal activity committed using computers and/or the internet. It is broadly categorised as either 'cyber-enabled' (crimes that happen off-line but are enabled at scale and at speed on-line) or 'cyber dependent' (crimes that can be committed only by using a computer). Cyber dependent crimes include:

- Unauthorised access to computers (illegal 'hacking'), for example accessing a school's computer network to look for test papers answers or change grades awarded
- Denial of service (Dos or DDoS) attacked or 'booting'. These are attempts to make a computer, network, or website unavailable by overwhelming it with internet traffic from multiple sources; and;
- Making, supplying, or obtaining malware (malicious software) such as viruses, spyware, ransomware, botnets, and remote access trojans with the intent to commit further offence, including those above.

4.3.2 We recognise that children with a particular skill or interest in computing and technology may inadvertently or deliberately stray into cyber-dependent crime. If there are concerns in this area Designated Safeguarding Leads should consider referring into the 'Cyber Choices' programme. This is a nationwide Police initiative supported by the Home Office and led by the National Crime Agency, working with regional and local policing. It aims to intervene where young people are at risk of committing, or being drawn into, low level cyber dependent offences and divert them to a more positive use of their skills and interests.

4.3.3 Additional advice can be found at: https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime/cyberchoices

4.4 Risk Assessment

4.4.1 As technology evolves, risks and harms can change rapidly, and it is for this reason that we require each school to routinely review their approach to online safety. This consideration should also be supported by an annual risk assessment, that has been appropriately localised and reflects the risks children face, and includes the safeguards in place to mitigate against these risks.

5 Curriculum context

5.1 Pupils are taught about online safety, and we consider this as part of providing a broad and balanced curriculum. This includes covering relevant issues through Relationships Education (for all primary pupils) and Relationships and Sex Education (for all secondary pupils) and Health Education. The statutory guidance can be found here: Statutory guidance: relationships education relationships and sex education (RSE) and health education.

5.2 The Department has produced a one-stop page for teachers on GOV.UK, which can be accessed here: Teaching about relationships sex and health. This includes teacher training modules on the RSHE topics and non-statutory implementation guidance. The following resources may also help schools and colleges understand and teach about safeguarding:

- DfE advice for schools: teaching online safety in schools;
- UK Council for Internet Safety (UKCIS) guidance: Education for a connected world;
- UKCIS guidance: Sharing nudes and semi-nudes: advice for education settings working with children and young people;
- The UKCIS external visitors guidance will help schools and colleges to ensure the maximum impact of any online safety sessions delivered by external visitors;
- National Crime Agency's CEOP education programme: Thinkuknow;
- Public Health England: Rise Above.

5.3 This work complements the computing curriculum, which covers the principles of online safety at all key stages, with progression in the content to reflect the different and escalating risks that pupils face. This includes how to use technology safely, responsibly, respectfully, and securely, and where to go for help and support when they have concerns about content or contact on the internet or other online technologies. There are also other curriculum subjects which include content relevant to teaching pupils how to use the internet safely. For example, citizenship education covers media literacy (distinguishing fact from opinion) as well as exploring freedom of speech and the role and responsibility of the media in informing and shaping public opinion. It also supports teaching about the concept of democracy, freedom, rights, and responsibilities.

5.4 Teaching about online safety

5.4.1 The online world develops and changes at great speed. New opportunities, challenges and risks are appearing all the time. This can make it difficult for schools to stay up to date with the latest devices, platforms, apps, trends, and related threats. It is therefore important to focus on the underpinning knowledge and behaviours that can help children and young people to navigate the online world safely and confidently regardless of the device, platform, or app.

5.4.2 Schools can help children consider questions including:

- Is this website/URL/email fake? How can I tell?
- What does this cookie do and what information am I sharing?
- Is this person who they say they are?
- Why does someone want me to see this?
- Why does someone want me to send this?
- Why would someone want me to believe this?

- Why does this person want my personal information?
- What is behind this post?
- Is this too good to be true?
- Is this fact or opinion?
- How to recognise techniques used for persuasion. This will enable pupils to recognise the techniques that are often used to persuade or manipulate others, understanding that a strong grasp of knowledge across many areas makes people less vulnerable to these techniques and better equipped to recognise and respond appropriately to strongly biased intent or malicious activity.

5.4.3 Schools can help children to recognise:

- Online content which tries to make people believe something false is true and/or mislead (misinformation and disinformation);
- Techniques that companies use to persuade people to buy something;
- Ways in which games and social media companies try to keep users online longer (persuasive/sticky design);
- Criminal activities such as grooming;
- Online behaviour, enabling pupils to understand what acceptable and unacceptable online behaviour look like. Schools should teach pupils that the same standard of behaviour and honesty apply on and offline, including the importance of respect for others. Schools should also teach pupils to recognise unacceptable behaviour in others.

5.4.4 Schools can help children to recognise acceptable and unacceptable behaviour by:

- Looking at why people behave differently online, for example how anonymity (you do not know me) and invisibility (you cannot see me) affect what people do, and how to disengage from unwanted contact or content online; and considering unacceptable online behaviours often passed off as so-called social norms or just banter, for example the negative language that can be used, and in some cases is often expected, as part of online gaming and the acceptance of misogynistic, homophobic and racist language that would never be tolerated offline.
- Enabling pupils to identify online risks and make informed decisions about how to act. This should not be about providing a list of what not to do online, the focus should be to help pupils assess a situation, think through the consequences of acting in different ways and decide on the best course of action.

5.4.5 Schools can help children to identify and manage risk by:

- Discussing the ways in which someone may put themselves at risk online
- Discussing risks posed by another person's online behaviour
- Discussing when risk taking can be positive and negative
- Discussing "online reputation" and the positive and negative aspects of an online digital footprint. This could include longer-term considerations, i.e how past online behaviours could impact on their future, place at university or a job for example.
- Looking at how online emotions can be intensified, resulting in mob mentality (influence of others to adopt certain behaviours on a largely emotional rather than rational basis)

- Teaching techniques (relevant on and offline) to defuse or calm arguments, for discussing the risks vs the benefits of sharing information online and how to make a judgement about when and how to share and who to share with
- Asking questions such as what might happen if I post something online? Who will see it? Who might they send it to?
- Enabling pupils to understand how and when to seek support if they are concerned or upset by something, they have seen online

5.4.6 Schools can help children by:

- Helping them to identify who trusted adults are
- Looking at the different ways to access support from the school, police, the National Crime Agency's Click CEOP reporting service for children and third sector organisations such as Childline and Internet Watch Foundation. This links to wider school policies and processes around reporting of safeguarding and child protection incidents and concerns to school staff (see Keeping Children Safe in Education)
- Helping them to understand that various platforms and apps will have ways in which inappropriate contact or content can be reported.

5.5 **Additional Considerations for Schools**

5.5.1 When planning their curriculum and how online safety fits within it, schools will carefully consider the following.

5.5.1.1 Vulnerable children – Any child can be vulnerable online, and their vulnerability can fluctuate depending on their age, developmental stage, and personal circumstance. However, there are some, for example looked after children and those with special educational needs, who may be more susceptible to online harm or have less support from family or friends in staying safe online. Schools should consider how they tailor their offer to ensure these pupils receive the information and support they need. The following resources can help schools consider how best to support their most vulnerable pupils stay safe online: Vulnerable Children in a Digital World - Internet Matters; Children's online activities, risks and safety - A literature review by the UKCCIS Evidence Group (section 11); STAR SEN Toolkit – Childnet.

5.5.1.2 Use of external resources – Schools are best placed to make their own decisions about which resources are educationally appropriate for their children. This includes reviewing resources, even when from a trusted source, as some will be more appropriate to their cohort of children than others. Requests for subscription services or licenses, should be made via IT Services, so that a central Trust license can be procured. Due considerations however should be made:

- Where does this organisation get their information from?
- What is their evidence base?
- Have they been externally quality assured?
- What is their background?
- Are the resources age appropriate for our pupils?
- Are the resources appropriate for the developmental stage of our pupils?
- Has the Data Protection Officer checked for GDPR compliance?

- Have IT Services checked for network compatibility?

5.5.1.3 Use of external visitors - Online safety can be a difficult and complex topic which changes very quickly. Therefore, schools may want to seek external support who have expertise, up-to-date knowledge and information. The right external visitors can provide a useful and engaging approach to deliver online safety messages, but this should enhance a school's offer rather than be delivered in isolation. The UK Council for Internet Safety has developed guidance for educational settings seeking support from external visitors to help explore issues such as cyberbullying, online pornography, 'sexting' and staying safe online. Schools can use this document to guide their process of selecting suitable visitors and sessions.

5.6 Whole School Approach

5.6.1 Whole school approaches are likely to make teaching more effective than lessons alone. A whole school approach is one that goes beyond teaching to include all aspects of school life, including culture, ethos, environment and partnerships with families and the community. Our schools will embed teaching about online safety and harms within a whole school approach. In practice, this means:

5.6.2 Creating a culture that incorporates the principles of online safety across all elements of school life. The principles should be reflected in the other policies and practice where appropriate, and should be communicated with staff, children, and parents/carers.

5.6.3 Proactively engaging staff, pupils and parents/carers in school activities that promote the agreed principles of online safety.

5.6.4 Reviewing and maintaining the online safety principles includes making sure that school staff have access to up-to-date and appropriate training/CPD and resources so that they are confident in covering the required content in a way that is relevant to their pupils' lives. It could also include using information available to the school to review practices and ensure the issues facing their pupils are covered in a timely manner.

5.6.5 Embedding the online safety principles when teaching curriculum subjects and through other teaching opportunities. Reinforcing what is taught in lessons by taking appropriate and consistent action when a child makes a report of unacceptable online behaviours from another pupil, including cyberbullying, or shares a concern about something they have seen online.

5.6.6 Modelling the online safety principles consistently. This includes expecting the same standards of behaviour whenever a child is online at school - be it in class, logged on at the library or using their own device in the playground or at home. Schools should also ensure they extend support to parents, so they are able to incorporate the same principles of online safety outside of school.

5.7 Remote education

5.7.1 It is important that we continue to provide a safe online environment for those who are required to continue to learn whilst at home (due to extenuating circumstances). It is important that all staff who interact with children, including online, continue to look out for signs a child may be at risk. Any such concerns should be dealt with as per the Trust safeguarding policy and where appropriate referrals should continue to be made to children's social care and, as required, the police.

5.7.2 The starting point for online teaching should be that the same principles as set out in the Tudor Grange Academies Trust Staff Code of Conduct should be followed. This policy includes, amongst other things, acceptable use of technologies, staff pupil/ relationships and communication including the use of social media. The policy should apply equally to any existing or new online and distance learning arrangements which are introduced. Staff must also read 'Guidance for safer working practice for those working with children and young people in education settings' before facilitating their first session.

5.7.3 We will continue to ensure any use of online learning tools and systems is in line with privacy and data protection requirements.

5.7.4 An essential part of the online planning process will be ensuring children who are being asked to work online have very clear reporting routes in place so they can raise any concerns whilst online. As well as reporting routes back to school, children can receive age-appropriate practical support from the likes of:

- Childline - for support
- UK Safer Internet Centre - to report and remove harmful online content
- CEOP - for advice on making a report about online abuse

5.7.5 Staff are likely to be in contact with parents and carers during this engagement. Those communications will continue to be used to reinforce the importance of children being safe online. It will be especially important for parents and carers to be aware of what their children are being asked to do online, including the sites they will asked to access and be clear who from the school (if anyone) their child is going to be interacting with online.

5.7.6 Parents and carers may choose to supplement the school online offer with support from online companies and in some cases individual tutors. In their communications with parents and carers, we will emphasise the importance of securing online support from a reputable organisation/individual who can provide evidence that they are safe and can be trusted to have access to children.

5.7.7 There is no expectation that teachers should live stream or provide pre-recorded videos, but those who do should ensure they have read and understood Trust guidance on conducting remote live sessions – see 'Tudor Grange Academies Trust Live Lessons' document.

5.7.8 Teaching from home is different to teaching in the classroom. Teachers should try to find a quiet or private room or area to talk to pupils, parents or carers. When broadcasting a lesson or making a recording, also consider what will be in the background and ensure that attire is appropriate. Guidance should be shared and agreed by pupils and their parents/carers with respect to them also observing appropriate online behaviours (location, attire etc) – see 'Tudor Grange Academies Trust Live Sessions – Home Communication' document.

5.7.9 **Further information**:

- The Data Protection Act 2018;
- Teaching Online Safety in School: Guidance to support schools to teach their pupils how to stay safe online, within new and existing school subject;
- Safeguarding Children and Protecting Professionals in Early Years Settings: Online Safety Considerations for Managers;
- Keeping Children Safe in Education.

6 Managing Information Systems

6.1 How will information systems security be maintained?

- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- School computer activity will be monitored through Impero and the use of Smoothwall reports, which will be regularly reviewed and acted upon by the safeguarding team.
- Personal data sent over the Internet or taken off site will be encrypted.
- Unapproved software will not be allowed in pupils' work areas or attached to email.
- Files held on the school's network will be regularly checked.
- Remote communication between pupils and staff because of remote learning or working arrangements will only take place via Microsoft Teams, as a secure platform. Communication via any other online platform is not permitted.
- The network manager will review system capacity regularly.

6.2 How will email be managed?

- Pupils may only use approved email accounts.
- Pupils must immediately tell a teacher if they receive offensive email.
- Pupils must not reveal personal details of themselves or others in email communication or arrange to meet anyone without specific permission from an adult.
- Access whilst in school to external personal email accounts may be blocked. Excessive social email use can interfere with learning and will be restricted.
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on Academy headed paper.
- The forwarding of chain messages is not permitted.
- Schools may have a dedicated email for reporting wellbeing and pastoral issues and this inbox must be approved and monitored by members of the Senior Leadership Team.
- Staff should only use Tudor Grange Academy email accounts to communicate with pupils as approved by the Senior Leadership Team.
- Staff should not use personal email accounts during school hours or for professional purposes.

6.3 How will published content be managed?

- The contact details on the website should be the Academy address, email, and telephone number. Staff or pupils' personal information must not be published.
- Email addresses should be published carefully, to avoid being harvested for spam (e.g. replace '@' with 'AT'.
- The website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright.

6.4 Can pupil images or work be published?

- Images that include pupils will be selected carefully and will not provide material that could be reused.

- Written permission from parents or carers will be obtained before images of pupils are electronically published.
- Pupil work will generally be restricted to the Virtual Learning Environment which will only be accessed by staff and pupils of the school. Exceptional work may be displayed on the public website. Again, images of the pupil concerned would need permission from the parents/carers.

6.5 **How will social networking, social media and personal publishing be managed?**

- TG IT Services control access to social media and social networking sites at all of our schools. We do understand the need for a social network as school is a place of social learning, however all external social media sites such as Facebook, Twitter, Bebo are blocked for pupils in our schools. Our own learning platform and Office 365 allow pupils to communicate and collaborate, but access to this is permission based and is filtered.
- Pupils are advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc. Pupils are advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the pupil or his/her location. If personal publishing is to be used with pupils, then it must use age appropriate sites suitable for educational purposes. Personal information must not be published, and the site should be moderated by school staff.
- Pupils are advised on security and encouraged to set passwords, deny access to unknown individuals, and instructed how to block unwanted communications. Pupils are also encouraged to invite known friends only and deny access to others by making profiles private. Pupils are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory. See Appendix 6 for guidance on how to report abuse on social media and Appendix 7 for young people's rights on social media.
- TG official social media sites

6.5.1 Some TG academies do have social media sites which are managed by Senior Leaders at our sites. These sites are setup by TG IT services only, who maintain admin access. Only the Head or Principal can approve creation of a social media site. Staff should be advised not to run social network spaces for student use on a personal basis. The purpose of these sites is broadcast only, used to market and showcase school activity.

6.5.2 TG academies do have official Twitter accounts which are controlled by managers at our Academies, but we have very strict rules regarding their use. The sole purpose of the official Twitter accounts is for schools and departments to provide information; it is strictly prohibited for staff to use it as a tool to communicate to communicate with students.

6.5.3 Student Regulations:

- Access to the official Twitter website is blocked onsite at our schools.
- Pupils are prohibited from using Twitter on mobile twitter devices and the application is blocked onsite via our web filter.
- Pupils are advised not follow Twitter accounts of unknown origin.

6.5.4 Staff Regulations:

- Staff are not permitted to use personal Twitter accounts for school business.
- Requests for official Twitter accounts must be made through TG IT Services with the approval of the Head / Principal.
- Official department accounts are monitored by TG IT Services.
- Staff are not permitted to add pupils as friends.
- All tweets must be made in the knowledge that they represent Tudor Grange Academies Trust and therefore must follow Trust policies.
- Personal information should not be published.

6.6 **How will filtering be managed?**

- The school will work with partner schools to ensure that systems to protect pupils are reviewed and improved. If staff or pupils discover unsuitable sites, the URL must be reported to TG IT Services.
- The school's broadband access will include filtering appropriate to the age and maturity of pupils.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective, and reasonable. Any material that the school believes is illegal must be reported to appropriate agencies such as IWF, CEOP, or directly to the police. The school's access strategy will be designed by educators to suit the age and curriculum requirements of the pupils, with advice from network managers. Smoothwall reports detailing any concerning online activity will be shared with the safeguarding team to ensure that any issues raised are followed up swiftly and safely.
- Whilst it is essential that we ensure that appropriate filters and monitoring systems are in place, we work to ensure that "over blocking" does not lead to unreasonable restrictions as to what pupils can be taught with regard to online teaching and safeguarding.

6.7 **How will video conferencing be managed?**

- Any staff undertaking remote video conferencing sessions with pupils must read and follow the 'Tudor Grange Academies Trust Live Lessons' guidance document.
- Parents/carers must consent to their child taking part in videoconferences
- When recording a video conference lesson, written permission should be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference. Recorded material shall be stored securely.
- All video conferencing equipment in the classroom must be switched off when not in use and not set to auto answer.
- Equipment connected to the educational broadband network should use the national E.164 numbering system and display their H.323 ID name.
- External IP addresses should not be made available to other sites.
- Videoconferencing contact information should not be put on the school website.

- The equipment must be secure and if necessary locked away when not in use.
- School videoconferencing equipment should not be taken off school premises without permission.

6.8 **How can emerging technologies be managed?**

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Staff will be issued with a school phone where contact with pupils is required.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text, picture or video messages is forbidden.
- The Trust will investigate wireless, infrared and Bluetooth communication technologies.

6.9 **How should personal data be protected?**

- Personal data will be recorded, processed, transferred, and made available according to the Data Protection Act 2018. No personal data will be taken off an Academy site unless in an encrypted form.

6.10 **How will computer activity be monitored and managed?**

6.10.1 School computers have Impero software installed. Impero is a classroom management and computer monitoring software. The software produces reports of inappropriate activity, and these reports are collated and dealt with regularly. The software has several e-safety features:

- prevent access to unsuitable sites
- prevent unauthorised use of proxy sites
- enforce acceptable usage policy
- create key word libraries for real-time detection
- monitor using specialist built-in key word libraries
- determine potential risk through key word glossaries with explanations
- create different policies depending on severity
- capture time stamped screen shots of every violation
- add screenshots to log viewer report
- record on-screen activity and specify recording length to capture misuse
- export violations with details and image to PDF
- evidence misconduct from a centralised log to support disciplinary action
- alert the relevant authority when rules are violated
- apply policies and filters to laptops when disconnected from the network
- log and monitor all web activity
- enable pupils to anonymously report concerns using the Confide system.

7 Breaches

7.1 A breach may arise from a theft, a deliberate attack on your systems, the unauthorised or malicious use of personal data by a member of staff, accidental loss, or equipment failure.

7.2 In addition:

- no school or individual would want to be the cause of a data breach, particularly as the impact of data loss on individuals can be severe, put individuals at risk and affect personal, professional or organisational reputation
- schools are "data rich" and the introduction of electronic storage and transmission of data has created additional potential for the loss of data
- the school will want to avoid the criticism and negative publicity that could be generated by any personal data breach

7.3 Schools have always held personal data on the learners in their care, and increasingly this data is held digitally and accessible not just in schools but also from remote locations. It is important to stress that the Data Protection Laws apply to all forms of personal data, regardless of whether it is held on paper or in electronic format. However, as it is part of an overall online safety policy template, this document will place particular emphasis on data which is held or transferred digitally.

7.4 Schools will need to carefully review their policy in the light of pertinent Local Authority regulations and guidance and changes in legislation.

7.5 All significant data protection incidents must be reported through the DPO to the Information Commissioner's Office based upon the local incident handling policy and communication plan. The new laws require that this notification should take place within 72 hours of the breach being detected, where feasible.

7.6 The school should have a policy for reporting, logging, managing, and recovering from information risk incidents, which establishes a:

- "responsible person" for each incident
- communications plan, including escalation procedure
- plan of action for rapid resolution
- plan of action of non-recurrence and further awareness raising

7.7 Privacy by Design and Data Protection Impact Assessments (DPIA)

7.7.1 Data Protection Impact Assessments (DPIA) identify and address privacy risks early on in any project so that you can mitigate them before the project goes live. DPIAs should be carried out by Data Managers (where relevant) under the support and guidance of the DPO. Ideally you should conduct a DPIA before processing activity starts. However, some may need to be retrospective in the early stages of compliance activity. The risk assessment will involve:

- recognising the risks that are present
- judging the level of the risks (both the likelihood and consequences)
- prioritising the risks.

7.7.2 According to the ICO a DPIA should contain:

- a description of the processing operations and the purpose

- an assessment of the necessity and proportionality of the processing in relation to the purpose
- an assessment of the risks to individuals
- the measures in place to address risk, including security and to demonstrate that you comply.

Or more simply and fully:

- who did you talk to about this?
- what is going to happen with the data and how – collection, storage, usage, disposal
- how much personal data will be handled (number of subjects)
- why you need use personal data in this way
- what personal data (including if it is in a 'special category') are you using
- at what points could the data become vulnerable to a breach (loss, stolen, malicious)
- what the risks are to the rights of the individuals if the data was breached
- what are you going to do in order to reduce the risks of data loss and prove you are compliant with the law.

7.8 DPIA is an ongoing process and should be re-visited at least annually to verify that nothing has changed since the processing activity started

8 Policy decisions

8.1 How will Internet access be authorised?

8.1.1 The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications. All staff and students must read and sign the 'Acceptable User Agreement' before using any school ICT resource (see Appendix 2), this is done via Impero, the first time a user logs on. Staff retain the right to turn Internet use off in a classroom if its use is a distraction to learning following abuse by pupils.

8.2 How will risks be assessed?

8.2.1 The school will take all reasonable precautions to ensure that user's access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via an school computer. The school can accept liability for the material accessed, or any consequences resulting from Internet use.

8.2.2 The school should audit ICT use to establish if the e–Safety policy is adequate and that the implementation of the e–Safety policy is appropriate. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990. Methods to identify, assess and minimise risks will be reviewed regularly.

8.3 How will e–Safety complaints be handled?

8.3.1 Complaints of Internet misuse will be dealt with under the school's Complaints Procedure. Any complaint about staff misuse must be referred to the Principal/Head of School. All e–Safety complaints and incidents will be recorded by the school — including any actions

taken. Pupils and parents/carers will be informed of the complaint's procedure. Parents/carers and pupils will work in partnership with staff to resolve issues.

8.3.2 Any issues (including sanctions) will be dealt with according to the school's disciplinary and safeguarding policies. Referrals to appropriate providers including the Police and Children's Social Care will also be considered as required.

8.4 How is the Internet used across the community?

8.4.1 The school will liaise with local organisations to establish a common approach to e–Safety. The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

8.5 How will cyberbullying be managed?

8.5.1 Cyberbullying (along with all forms of bullying) will not be tolerated. Full details are set out in the school's policy on anti-bullying. There will be clear procedures in place to support anyone affected by cyberbullying. All incidents of cyberbullying reported to the school will be recorded. There will be clear procedures in place to investigate incidents or allegations of cyberbullying: Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence. The school will take steps to identify the bully, where appropriate, such as examining system logs, identifying, and interviewing possible witnesses, and contacting the service provider and the police, if necessary. Sanctions for those involved in cyberbullying may include:

- Pupils will be asked to remove any material deemed to be inappropriate or offensive.
- A service provider may be contacted to remove content.
- Internet access may be suspended at school for the user for a period.
- Parents/carers may be informed.
- Sanctions in line with the Behaviour Policy.
- The Police will be contacted if a criminal offence is suspected.

8.6 How will Learning Platforms and learning environments be managed?

8.6.1 SLT and staff will monitor the usage of all school learning platforms and virtual learning environments, by pupils and staff regularly in all areas, in particular message and communication tools and publishing facilities. Pupils/staff will be advised on acceptable conduct and use when using these online environments. Only members of the current pupils, parent/carers and staff community will have access to Tudor Grange Academy learning environments. All users will be mindful of copyright issues and will only upload appropriate content. When staff or pupils leave the school their account or rights to specific school areas will be disabled or transferred to their new establishment. Any concerns with content may be recorded and dealt with in the following ways:

- The user will be asked to remove any material deemed to be inappropriate or offensive.
- The material will be removed by the site administrator if the user does not comply.
- Access to Tudor Grange Academy learning environments for the user may be suspended.
- Sanctions in line with behaviour policy used.
- The user will need to discuss the issues with a member of SLT before reinstatement.

- A pupil's parent/carer may be informed.
- A visitor (such as an exam moderator) may be invited onto the learning platform by a member of the SLT. In this instance there may be an agreed focus or a limited time slot.
- Pupils may require editorial approval from a member of staff. This may be given to the pupil to fulfil a specific aim and may have a limited time frame.

9 Awareness and Communication

9.1 How will the policy be shared with pupils?

9.1.1 All users will be informed that network and Internet use will be monitored. Pupil instruction in responsible and safe use should precede Internet access. E–Safety will be included in the curriculum, for example through IT, PSHE and/or Relationships Education, covering both safe school and home use. Safe and responsible use of the Internet and technology will be reinforced across the curriculum. Particular attention will be given where pupils are considered to be vulnerable. A desktop link to the e-Safety site for the school will be available via Magellan. The school acknowledges, learns from, and uses the skills and knowledge of learners in the use of digital technologies. We recognise the potential for this to shape the online safety strategy for the school community and how this contributes positively to the personal development of young people. Their contribution is recognised through:

- mechanisms to canvass learner feedback and opinion.
- appointment of digital leaders/anti-bullying ambassadors/peer mentors
- the Online Safety Group has learner representation
- learners contribute to the online safety education programme e.g. peer education, digital leaders leading lessons for younger learners, online safety campaigns
- learners designing/updating acceptable use agreements
- contributing to online safety events with the wider school community e.g. parents' evenings, family learning programmes etc.

9.2 How will the policy be discussed with staff?

9.2.1 The e–Safety Policy will be formally provided to and discussed with all members of staff. To protect all staff and students, the school will implement Acceptable Use Policies. Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct from all staff is essential. All staff will 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 and data protection training will be made available to all staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- the training will be an integral part of the school's annual safeguarding and data protection training for all staff
- all new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use

agreements. It includes explicit reference to classroom management, professional conduct, online reputation, and the need to model positive online behaviours

- the Online Safety Lead and Designated Safeguarding Lead (or other nominated person) will receive regular updates through attendance at external training events, (e.g. UKSIC / SWGfL / MAT / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations
- the Online Safety Lead (or other nominated person) will provide advice/guidance/training to individuals as required.

9.3 **How will parents' support be enlisted?**

9.3.1 Parents'/carers' attention will be drawn to the school e–Safety Policy in newsletters, the school brochure and on the school website. A partnership approach with parents/carers will be encouraged. This could include parent evenings with demonstrations and suggestions for safe home Internet use or highlighting e–Safety at other attended events e.g. parent evenings.

9.3.2 Parents/carers will be requested to sign an e–Safety/internet agreement as part of the Home School Agreement. Information and guidance for parents/carers on e–Safety will be made available in a variety of formats. Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents/carers. Interested parents/carers will be referred to organisations listed in Appendix 1.

9.3.3 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.

9.3.4 The school will seek to provide information and awareness to parents and carers through regular communication, awareness-raising and engagement on online safety issues, curriculum activities and reporting routes such as:

- regular opportunities for engagement with parents/carers on online safety issues through awareness workshops / parent/carer evenings etc
- the learners – who are encouraged to pass on to parents the online safety messages they have learned in lessons and by learners leading sessions at parent/carer evenings.
- letters, newsletters, website, learning platform,
- high profile events / campaigns e.g. Safer Internet Day
- reference to the relevant web sites/publications, e.g. SWGfL; http://www.saferinternet.org.uk/; http://www.childnet.com/parents-and-carers (see Appendix for further links/resources).
- Sharing good practice with other schools in clusters and or the local authority/MAT

Appendix 1: e-Safety Information, Advice and Support

There is a wealth of information available to support schools, colleges, and parents to keep children safe online. The following list is not exhaustive but should provide a useful starting point:

Support for parents and carers.

- Internet Matters – a not-for-profit organisation set up to empower parents and carers to keep children safe in the digital world. Their support for parents includes a range of downloadable guides covering subjects such as transition to secondary school, Vlogging & livestreaming, online gaming and cyberbullying.
- NSPCC - includes a range of resources to help parents keep children safe when they're using the internet, social networks, apps, games and more.
- Parent Info - from CEOP and Parent Zone, Parent Info is a website for parents covering all the issues amplified by the internet. It is a free service which helps schools engage parents with expert safety advice, endorsed by the National Crime Agency's CEOP command. This website provides expert information across a range of online harms.
- Parent Zone - offers a range of resources for families, to help them meet the challenges of the digital age, including parent guides on the latest digital trends and platforms.
- Common Sense Media - Independent reviews, age ratings, & other information about all types of media including games, apps, films and books.
- Let's Talk About It has advice for parents and carers to keep children safe from online radicalisation.
- Childnet offers a toolkit to support parents and carers of children of any age to start discussions about their online life, to set boundaries around online behaviour and technology use, and to find out where to get more help and support
- London Grid for Learning has support for parents and carers to keep their children safe online, including tips to keep primary aged children safe online

Support for children and young people

- BBC Own It – Support for young people to take control of their online life, including help and advice, skills and inspiration on topics such as friendships and bullying, safety and self-esteem. Free app available.
- Childline – includes information for pupils on sexting, gaming, grooming, bullying, porn, relationships.
- Childline/IWF Report Remove is a free tool that allows children to report nude or sexual images and/or videos of themselves that they think might have been shared online
- Report Harmful Content - https://reportharmfulcontent.com/
- Think U Know – age appropriate advice for staying safe when using a tablet, mobile phone or computer.
- Disrespect Nobody - Home Office advice on healthy relationships, including sexting and pornography

Support and Resources for Schools: Government Guidance

- Keeping Children Safe in Education - Statutory guidance for schools and colleges on safeguarding children and safer recruitment.
- Teaching online safety in schools - DfE advice outlining how schools can ensure their pupils understand how to stay safe and behave online as part of existing curriculum requirements.
- Behaviour and discipline in schools - Guidance for school leaders and staff on developing a school behaviour policy, and a checklist of actions to take to encourage good behaviour.
- Searching, screening and confiscation at school - Guidance explaining the powers schools have to screen and search pupils, and to confiscate items they find.
- educateagainsthate - Practical advice for parents, teachers and governors on protecting children from extremism and radicalisation.
- The use of social media for online radicalisation - A briefing note for schools on how social media is used to encourage travel to Syria and Iraq.
- CEOP Think U Know Programme: Online safety education programme from the National Crime Agency's CEOP Command which aims to safeguard children from sexual abuse and exploitation. Education resources and online advice for children aged 4 – 18, expert and support and professional development for the children's workforce. Signposts to the NCA's Click CEOP service for children to report concerns related to sexual abuse.
- National Centre for Computing Education (NCCE) has been set up to support the teaching of computing education throughout schools and colleges in England, giving teachers the subject knowledge and skills to establish computing as a core part of the curriculum. To help primary and secondary schools teach the safety and security aspects of the National Curriculum Computing Programme of Study, the National Centre for Computing Education's resource repository and professional development courses cover objectives from the Education for Connected World framework. The resource repository's lesson plans will include links to the framework, as well as specific activities for non-specialist teachers.
- UK Council for Internet Safety - The UK Council for Internet Safety expands the scope of the UK Council for Child Internet Safety to achieve a safer online experience for all users, particularly groups who suffer disproportionate harms. The website has useful resources for schools and parents to help keep children safe online including: Education for a Connected World – a framework describes the Digital knowledge and skills that children and young people should have the opportunity to develop at different ages and stages of their lives. It highlights what a child should know in terms of current online technology, its influence on behaviour and development, and what skills they need to be able to navigate it.
- UK Chief Medical Officers' advice for parents and carers on children and young people's screen and social media use, published February 2019.

National Organisations: Support, Resources and Training for Schools

- National Online Safety – Specialist online safety training courses for school staff, parents and children along with resources for use in the classroom.

- The Anti-Bullying Alliance - A coalition of organisations and individuals, working together to stop bullying and create safer environments in which children and young people can live, grow, play and learn. Their website includes a range of tools and resources to support schools prevent and tackle cyberbullying.
- Childnet - a children's charity and has a wide range of practical resources freely available, covering all online safety issues, and which are available for teachers working with children of all ages, including children with SEN.
- The Diana Award – a charity running a number of different projects aimed at reducing bullying in schools. Their resource section has information to help schools tackle cyberbullying along with resources from their Be Strong Online Ambassador programme – a peer-led initiative which aims to empower young people to increase the digital resilience of their peers.
- DotCom Digital - a free resource for schools, created by children with Essex Police and the National Police Chief Council Lead for Internet Intelligence and Investigations, to be launched October 2019. The resource aims to prevent young people becoming victims of online grooming, radicalisation, exploitation and bullying by giving them the confidence to recognise warning signs and reach out to an adult for help.
- The Hopes and Streams report by London Grid for Learning has themed chapters that include links to online resources and ideas for tackling the issues raised.
- Internet Matters – a not-for-profit organisation set up to empower parents and carers to keep children safe in the digital world, they also have a dedicated section of their website for professionals which includes resources to support staff training, whole school programmes and policies and a parent pack to help schools engage with parents about online safety.
- Internet Watch Foundation – an internet hotline for the public and IT professionals to report potentially criminal online content, including child sexual abuse images online.
- NSPCC learning – includes a range of safeguarding and child protection teaching resources, advice and training for schools and colleges.
- Parent Zone's dedicated school zone - includes a range of resources to support teachers educate their pupils on how to stay safe online, what to do if they find themselves in an uncomfortable situation and how to build their digital resilience.
- PSHE Association - the national body for Personal, Social, Health and Economic (PSHE) education. Their programme of study for PSHE education aims to develop skills and attributes such as resilience, self-esteem, risk-management, team working and critical thinking. They also have many guides about how to teach specific topics.
- UK Safer Internet Centre –a partnership between Childnet International, Internet Watch Foundation and SWGfL to promote the safe and responsible use of technology for young people. Their website includes a range of practical resources and support for schools including: 360 degree safe - a free to use self-review tool for schools to assess their wider online safety policy and practice. A Helpline – This helpline was established to support those working with children across the UK with online safety issues. Operated by SWGfL, it can be contacted at 0344 381 4772 and helpline@saferinternet.org.uk. Safer Internet Day - The UK Safer Internet Centre organise Safer Internet Day for the UK and each year develops a range of materials from assemblies to lesson plans, posters to quizzes, for each Key Stage, to address a key online safety issue.

- Be Internet Legends - Be Internet Legends from Google and Parentzone a free internet safety curriculum with PSHE accredited lesson plans and teaching resources for Key Stage 2 pupils

Appendix 2: Staff (and Volunteer) Acceptable Use Policy Agreement

This acceptable use policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal, and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that learners receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate, or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images unless I have permission to do so. Where these images are published (e.g., on the school

website/VLE) it will not be possible to identify by name, or other personal information, those who are featured.

- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with learners and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices in school, I will follow the rules set out in this agreement, in the same way as if I were using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up-to-date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school's ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download, or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.
- I understand that data protection policy requires that any staff or learner data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software however this may have happened.

When using the online systems in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this acceptable use policy applies not only to my work and use of school's digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors/Trustees and/or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer Name: .....

Signed: .....

Date:.....

Appendix 3: Pupil Acceptable Use Policy Agreements

Acceptable Use Agreement for 6th Form Learners

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:

- I understand that the schools will monitor my use of the systems, devices, and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger" when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school's systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school's systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive, or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will only use my own personal devices (mobile phones/USB devices etc.) in school if I have permission. I understand that, if I do use my own devices in the school, I will follow

the rules set out in this agreement, in the same way as if I were using school equipment.

- I understand the risks and will not try to upload, download, or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software; however, this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person/organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will only use social media sites with permission and at the times that are allowed.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not try to download copies (including music and videos).
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be online-bullying, use of images or personal information).
- I understand that if I fail to comply with this acceptable use agreement, I may be subject to disciplinary action. This could include loss of access to the school network/internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections on the next page to show that you have read, understood, and agree to the rules included in the acceptable use agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

Learner Acceptable Use Agreement Form

This form relates to the learner acceptable use agreement; to which it is attached.
Please complete the sections below to show that you have read, understood, and agree to the rules included in the acceptable use agreement. If you do not sign and return this agreement, access will not be granted to school systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school's systems and devices (both in and out of school)
- I use my own devices in the school (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc.
- I use my own equipment out of the school in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school email, VLE, website etc.

Name of Learner: .....

Group/Class: .....

Signed: .....

Date:.....

Acceptable Use Agreement for Key Stage 3 & 4 Learners

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:

- I understand that the schools will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school's systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school's systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will only use my own personal devices (mobile phones/USB devices etc.) in school if I have permission. I understand that, if I do use my own devices in the school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.

- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software; however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person/organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will only use social media sites with permission and at the times that are allowed.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be online-bullying, use of images or personal information).
- I understand that if I fail to comply with this acceptable use agreement, I may be subject to disciplinary action. This could include loss of access to the school network/internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the acceptable use agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

Learner Acceptable Use Agreement Form

This form relates to the learner acceptable use agreement; to which it is attached.

Please complete the sections below to show that you have read, understood and agree to the rules included in the acceptable use agreement. If you do not sign and return this agreement, access will not be granted to school systems. I have read and understand the above and agree to follow these guidelines when:

- I use the school's systems and devices (both in and out of school)
- I use my own devices in the school (when allowed) e.g., mobile phones, gaming devices USB devices, cameras etc.
- I use my own equipment out of the school in a way that is related to me being a member of this school e.g., communicating with other members of the school, accessing school email, VLE, website etc.

Name of Learner: .....

Group/Class: .....

Signed: .....

Date:.....

Acceptable Use Agreement for Key Stage 2 Learners

This acceptable use agreement is intended:

- to ensure that learners will have good access to devices and online content, be responsible users and stay safe while using digital technologies for educational, personal, and recreational use
- to help learners understand good online behaviours that they can use in school, but also outside school
- to protect school devices and networks from accidental or deliberate misuse that could put the security of the systems and users at risk.
- When I use devices, I must behave responsibly to help keep me and other users safe online and to look after the devices.

For my own personal safety:

- I understand that what I do online will be supervised and monitored and that I may not be allowed to use devices in school unless I follow these rules and use them responsibly
- I will only visit internet sites that adults have told me are safe to visit
- I will keep my username and password safe and secure and not share it with anyone else
- I will be aware of "stranger danger" when I am online
- I will not share personal information about myself or others when online
- If I arrange to meet people off-line that I have communicated with online, I will do so in a public place and take a trusted adult with me
- I will immediately tell an adult if I see anything that makes me feel uncomfortable when I see it online.

I will look after the devices I use, so that the school and everyone there can be safe:

- I will handle all the devices carefully and only use them if I have permission.
- I will not try to alter the settings on any devices or try to install any software or programmes.
- I will tell an adult if a device is damaged or if anything else goes wrong.
- I will only use the devices to do things that I am allowed to do.
- I will think about how my behaviour online might affect other people:
- When online, I will act as I expect others to act toward me.
- I will not copy anyone else's work or files without their permission.
- I will be polite and responsible when I communicate with others, and I appreciate that others may have different opinions to me.
- I will not take or share images of anyone without their permission.

I know that there are other rules that I need to follow:

- I will only use my own personal devices (mobile phones/USB devices etc.) in the school if I have permission. If I am allowed, I still have to follow all the other school rules if I use them.

- I will only use social media sites with permission and at the times that are allowed
- Where work is protected by copyright, I will not try to download copies (including music and videos).
- When I am using the internet to find information, I should take care to check that the information is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.
- I should have permission if I use the original work of others in my own work.

I understand that I am responsible for my actions, both in and out of school:

- I know that I am expected to follow these rules in school and that I should behave in the same way when out of school as well.
- I understand that if I do not follow these rules, I may be subject to disciplinary action. This could include loss of access to the school network/internet, detentions, suspensions, parents/carers contacted and in the event of illegal activities involvement of the police.

Learner Acceptable Use Agreement Form

Please complete the sections below to show that you have read, understood, and agree to the rules included in the acceptable use agreement. If you do not sign and return this agreement, access will not be granted to school systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)
- I use my own devices in the school (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc.
- I am out of school and involved in any online behaviour that might affect the school or other members of the school.

Name of Learner: .....

Group/Class: .....

Signed: .....

Date:.....

Acceptable Use Agreement for Key Stage 1 Learners.

This acceptable use agreement is intended:

- to ensure that learners will have good access to devices and online content, be responsible users and stay safe while using digital technologies for educational, personal, and recreational use
- to help learners understand good online behaviours that they can use in school, but also outside school
- to protect school devices and networks from accidental or deliberate misuse that could put the security of the systems and users at risk.

Acceptable Use Agreement

When I use devices, I must behave responsibly to help keep me and other users safe online and to look after the devices.

For my own personal safety:

- I understand that what I do online will be supervised and monitored and that I may not be allowed to use devices in school unless I follow these rules and use them responsibly
- I will only visit internet sites that adults have told me are safe to visit
- I will keep my username and password safe and secure and not share it with anyone else
- I will be aware of "stranger danger" when I am online
- I will not share personal information about myself or others when online
- If I arrange to meet people off-line that I have communicated with online, I will do so in a public place and take a trusted adult with me
- I will immediately tell an adult if I see anything that makes me feel uncomfortable when I see it online.

I will look after the devices I use, so that the school and everyone there can be safe:

- I will handle all the devices carefully and only use them if I have permission.
- I will not try to alter the settings on any devices or try to install any software or programmes.
- I will tell an adult if a device is damaged or if anything else goes wrong.
- I will only use the devices to do things that I am allowed to do.
- I will think about how my behaviour online might affect other people:

When online, I will act as I expect others to act toward me.

- I will not copy anyone else's work or files without their permission.
- I will be polite and responsible when I communicate with others, and I appreciate that others may have different opinions to me.
- I will not take or share images of anyone without their permission.

I know that there are other rules that I need to follow:

- I will only use my own personal devices (mobile phones/USB devices etc.) in the school if I have permission If I am allowed, I still must follow all the other school rules if I use them.
- I will only use social media sites with permission and at the times that are allowed.
- Where work is protected by copyright, I will not try to download copies (including music and videos).
- When I am using the internet to find information, I should take care to check that the information is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.
- I should have permission if I use the original work of others in my own work.

I understand that I am responsible for my actions, both in and out of school:

- I know that I am expected to follow these rules in school and that I should behave in the same way when out of school as well.
- I understand that if I do not follow these rules, I may be subject to disciplinary action. This could include loss of access to the school network/internet, detentions, suspensions, parents/carers contacted and in the event of illegal activities involvement of the police.

Learner Acceptable Use Agreement Form

Please complete the sections below to show that you have read, understood, and agree to the rules included in the acceptable use agreement. If you do not sign and return this agreement, access will not be granted to school systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)
- I use my own devices in the school (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc.
- I am out of school and involved in any online behaviour that might affect the school or other members of the school.

Name of Learner: .....

Group/Class: .....

Signed: .....

Date:.....

Acceptable Use Agreement for Foundation and entry level Key Stage 1 Learners.

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers/tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of computers/tablets and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I break the rules, I might not be allowed to use a computer/tablet

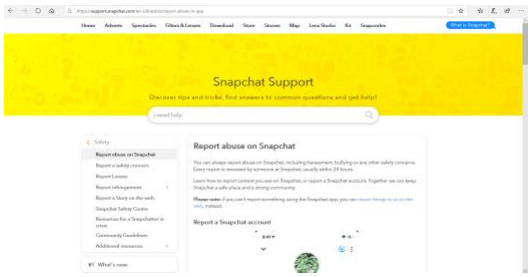
Signed (child): .....

Signed (parent): .....

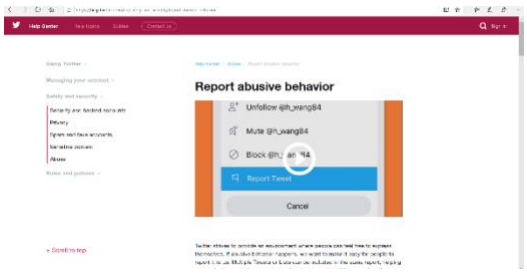
Appendix 4: How to Report Abuse on Social Media

Click on the following images to find guidance on each social media platform.

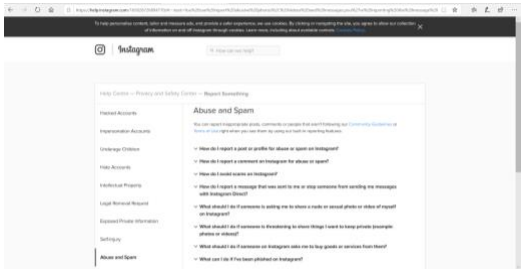
Snapchat:



Twitter:

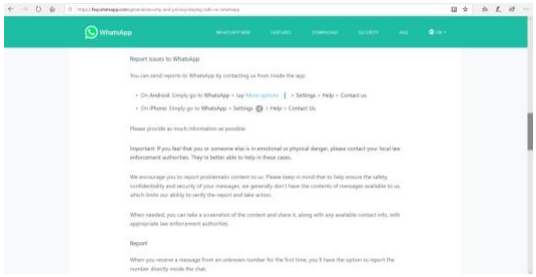


Instagram:

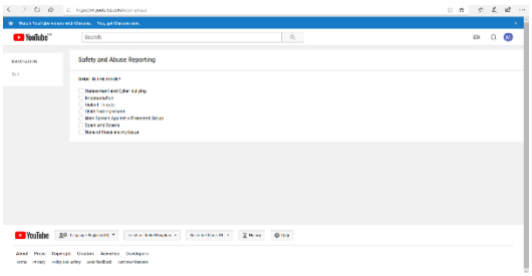


Facebook:

WhatsApp:



YouTube:



Appendix 5: Young People's Rights on Social Media

The Children's Commissioner has worked with lawyers to create simplified versions of terms and conditions for the most popular social media platforms. These guides are designed to give children more power and information online and help them know what they're signing up to when they join social media.

Young People's Rights on Facebook

Young People's Rights on Instagram

Young People's Rights on Snapchat

Young People's Rights on WhatsApp

Young People's Rights on YouTube