E-SAFETY POLICY

Role	*Designated Teacher for E-Safety*	*Deputy Designated Teacher*
Name	*Nevita Pandya*	*Mrs K Anderson*
Contact via	*Head Teachers office* *Main school office* *Tel 0208-304-8311*	*Head Teacher's office* *Main school office* *Tel 0208-304-8311*

Our 'Named Governor' with special responsibility for E-Safety is Mr J Paterson

Policy Reviewed & Approved by Governors:

Signed by Headteacher
Mr Desmond Deehan: _____

Signed on behalf of the Governors: _____

Date: _____November 2015_____

Contents

Introduction

New technologies are dynamic tools for learning and communication that can be used in school to enhance the curriculum, challenge students, and support creativity and independence. The internet and related communications technologies have become an integral part of young people's lives and therefore it is important that we educate our school community about the benefits and dangers they bring. Whilst children are confident with the technology, they are still developing critical evaluation skills and need our help to make wise decisions.

The requirements to ensure that young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work at Townley Grammar School are bound. Our school E-Safety Policy will help to ensure safe and appropriate use. The development and implementation of e-safety strategies is everybody's responsibility and involves all the stakeholders in a student's education from the Headteacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the students themselves.

The Byron Review, published in March 2008, made a number of recommendations about how we can improve children's safety in the digital world. The review emphasises the gap between what parents think they understand about digital safety, and what their children know -

"It is apparent that there is a big difference between what concerned parents understand and what their technologically savvy children know. Mobile phones and the internet have reached virtual ubiquity in the UK, but many parents and children are still unclear about the risks that these technologies pose. Mobile computing takes the risks associated with the internet outside of the home and away from easy parental oversight. The risks posed by the internet and mobile devices are not new. They are the risks children have always faced (and will continue to face in the future), and are a product of society. These risks have evolved with new technology and the internet, they now manifest in new ways and bring new challenges."

(Byron Review – Children and New Technology – Dr Tanya Byron)

The review argues that in order to support and, as necessary, protect children online we must reduce the availability of harmful content, minimise the access to such content, and equip students well so they can deal with exposure to harmful and inappropriate content and contact in a mature and sensible way.

The breadth of issues classified within e-safety is considerable, but can be categorised into three areas of risk:

Content: being exposed to illegal, inappropriate or harmful material

- exposure to inappropriate content, including online pornography; ignoring age ratings in games (exposure to violence, often associated with racist language); substance abuse and 'revenge porn'
- lifestyle websites, for example pro-anorexia, self-harm or suicide sites, hate sites
- content validation: how to check authenticity and accuracy of online content.

Contact: being subjected to harmful online interaction with other users

- grooming, cyber-bullying in all forms and identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords.

Conduct: personal online behaviour that increases the likelihood of, or causes, harm

- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being (amount of time spent online (internet or gaming))
- sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)
- copyright (little care or consideration for intellectual property and ownership – such as music and film).

(Inspecting E-Safety in Schools, September 2014, Ofsted)

Many of these risks reflect situations in the off-line world and it is vital that this E-Safety policy is used in conjunction with other school policies (e.g. Behaviour, Anti-Bullying and Safeguarding). As with all threats, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision, to build students' resilience to the dangers to which they may be exposed, to ensure they are empowered to manage these risks and make their digital world safer.

It is important that there is a balance between controlling access to the internet and technology and allowing freedom to explore and use these tools to their full potential. This policy aims to be an aid in regulating ICT activity in school, and provide a good understanding of appropriate ICT use that members of the school community can use as a reference for their conduct online outside of school hours. E-safety is a whole-school issue and responsibility.

Purpose, Aims & Scope

Townley Grammar School aims to educate staff, students and the wider community to use ICT as an effective and efficient teaching, learning, communication and management tool throughout the school.

The purpose of this policy is to set out the procedures by which the school will minimise the misuse of computers and associative technology -

- ✓ To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.
- ✓ To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to the student or liability to the school.
- ✓ E-Safety education (for students) and training (for staff, parents and governors) throughout the school is planned and up to date and appropriate to the recipients.
- ✓ To ensure that the school acts within the requirements of the Data Protection Act 1998 when retaining and storing personal data.
- ✓ All e-safety incidents will be dealt with promptly and appropriately.

This e-safety policy has been developed in consultation with the E-Safety Committee made up of:

- Senior Leadership Team
- Link governor for e-safety
- E-Safety Coordinator
- DHT responsible for Safeguarding
- Curriculum Leader for Computing
- Network Manager
- Student council representatives/ E-safety Mentors
- Parents/carers

Consultation with the whole school community has taken place through a range of formal and informal methods; (staff meetings, student council, CPD sessions, governors' meetings, parents evening and school website and newsletters.

The implementation of this E-Safety Policy is monitored by the:

- Senior Leadership Team
- E-safety Committee
- Curriculum Leaders
- Learning Managers
- Governors

The Governing Body will receive a report on the implementation of the E-Safety policy generated by this group (which will include anonymous details of E-Safety incidents) annually.

The school will monitor the impact of the policy using:

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

The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place.

Should serious e-safety incidents take place, the Safeguarding Lead, the Headteacher and the police will be informed.

Scope of the Policy

This policy applies to all members of the Townley Grammar School community (including staff, students, volunteers, parents / carers, visitors, and community users) who have access to and are users of school ICT systems, both in and out of the school.

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

Townley Grammar School will deal with such incidents within this policy and associated Behaviour and Anti-Bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Roles and Responsibilities - Appendix 1

The following personnel will be involved in the responsibility of e-safety at Townley Grammar School. Further details of their role and responsibilities can be found in **Appendix 1 Role & Responsibilies for E-Safety**.

- ✓ Governors
- ✓ Headteacher & Senior Leadership Team
- ✓ E-Safety Coordinator
- ✓ Network Manager & Technical staff
- ✓ Teaching and Support Staff
- ✓ Safeguarding Designated Person
- ✓ E-Safety Committee
- ✓ Students
- ✓ Parents & Carers

Education & Training - Appendix 2

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in e-safety is therefore an essential part of the school's e-safety provision. Young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

Many parents and carers have only a limited understanding of e-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 on-line 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.

It is essential that all staff, including teaching and support staff and governors receive e-safety training and understand their responsibilities, as outlined in this policy. Further details of education and training for students, parents, and staff can be found in **Appendix 2 Education & Training**.

Technical – Infrastructure, Hardware & Software - Appendix 3

The school will be responsible for ensuring that the school infrastructure is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people will be effective in carrying out their e-safety responsibilities. A more detailed Technical Security Policy can be found in **Appendix 3 Infrastructure.**

Policies to Support E-Safety – Appendix 4

To ensure safe use of the variety of technologies and tools available to staff and students a number of supporting 'sub-policies' are needed to support e-safety. These can be found in Appendix 4 and include –

- Cyberbullying
- Social Media
- Staff Acceptable Use Policy
- Student Acceptable Use Policy
- Data Protection
- Bring Your Own Device Policy
- Data Protection
- Use of digital/video images

Use of Communication Technologies

A wide range of rapidly developing communications technologies have the potential to enhance learning. The following table illustrates what the school considers acceptable for both students and staff with the use of mobile devices and other communication technologies such as email and social media:

Communication Technologies	Staff and other adults				Students				
	Not Allowed	Allowed at certain times	Allowed for selected staff	Allowed	Not Allowed	Allowed at certain times	Allowed in certain areas	Allowed with staff permission	Allowed
Mobiles may be brought into school				✓					✓
Mobile devices used in timetabled activities/school trips		✓						✓	
Mobile devices used appropriately in social time				✓			✓		
Taking photos on personal mobile devices of students and/or staff	✓				✓				
Use of personal email accounts through school network				✓				✓	
Use of school email for personal use	✓				✓				
Use of messaging apps on school devices	✓				✓				
Use of Social Media on school devices	✓				✓				
Use of blogs				✓				✓	

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report, to the nominated person, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

- Any digital communication between staff and students or parents / carers (email, chat, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Students will be provided with individual school email addresses for educational use.
- Students should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Unsuitable / inappropriate activities

Some internet activity eg accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities eg cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts usage as follows:

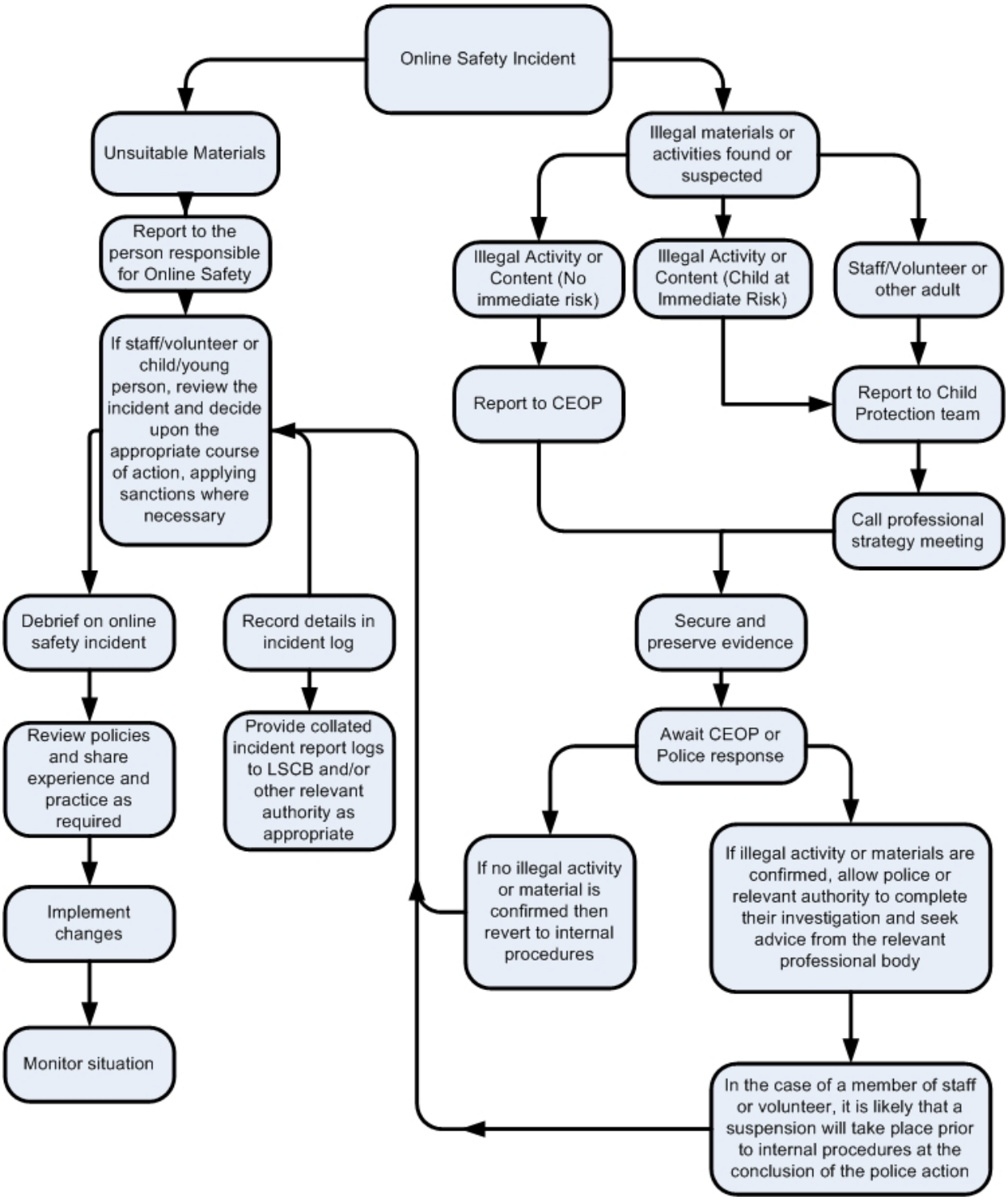
Some user actions listed below will also be **illegal** according to current legislation. Also refer to Staff Disciplinary Procedures.		Unacceptable	Acceptable at certain times	Acceptable for nominated users
Users shall not visit web sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images	✓		
	Promotion or conduct of illegal acts (e.g. under the child protection, obscenity, computer misuse & fraud legislation)	✓		
	Adult material that potentially breaches the obscene publications act in the UK	✓		
	Criminally racist material	✓		
	Pornography	✓		
	Promotion of any kind of discrimination	✓		
	Promotion of religious or racial hatred	✓		
	Threatening behaviour including promotion of physical violence or mental	✓		
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings it into disrepute	✓		
Using school systems to run a private business		✓		
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school		✓		
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions		✓		
Revealing or publicising confidential or proprietary information (e.g. financial/ personal information, databases, computer/ network access codes and passwords)		✓		
Creating or propagating computer viruses or other harmful files		✓		
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)				✓
On-line gaming (educational)			✓	
On-line gaming (non-educational)		✓		
On-line gambling		✓		
On-line shopping/commerce			✓	
Use of video broadcasting e.g. Youtube				✓

Responding to incidents of misuse – including illegal incidents

It is envisaged that all members of the school community will understand and follow this policy and hence be responsible users of new technologies. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely through deliberate misuse.

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above).

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.


Online Safety Incident
Unsuitable Materials
Illegal materials or activities found or suspected
Report to the person responsible for Online Safety
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Debrief on online safety incident
Record details in incident log
Secure and preserve evidence
Review policies and share experience and practice as required
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Await CEOP or Police response
Implement changes
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
Monitor situation
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

Other Incidents

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

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

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

- **If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**

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

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

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

School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal disciplinary procedures as follows:

Staff	Actions / Sanctions							
Incidents:	Disciplinary action	Suspension	Warning	Refer to line manager	Refer to Headteacher	Refer to HR	Refer to Technical Support Staff for action re filtering etc	Refer to Police
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	✓	✓	✓		✓	✓	✓	✓
Inappropriate personal use of the internet / social media / personal email			✓	✓	✓			
Unauthorised downloading or uploading of files			✓	✓	✓		✓	
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account			✓	✓	✓		✓	
Careless use of personal data eg holding or transferring data in an insecure manner			✓	✓	✓			
Deliberate actions to breach data protection or network security rules	✓		✓	✓	✓			
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	✓		✓	✓	✓			
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	✓			✓	✓		✓	
Using personal email / social networking / instant messaging / text messaging to carry out digital communications with students	✓			✓	✓		✓	
Actions which could compromise the staff member's professional standing	✓			✓	✓			
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school / academy	✓		✓	✓	✓			
Using proxy sites or other means to subvert the school's / academy's filtering system	✓				✓		✓	
Accidentally accessing offensive or pornographic material and failing to report the incident			✓		✓		✓	
Deliberately accessing or trying to access offensive or pornographic material	✓				✓		✓	✓
Breaching copyright or licensing regulations			✓	✓	✓		✓	
Continued infringements of any of the above, following previous warnings or sanctions	✓				✓			

Students	Actions / Sanctions									
Incidents:	**Refer to class teacher / tutor**	**Refer to ALM**	**Refer to SLT Link**	**Refer to Headteacher / E-Safety Co-ordinator**	**Refer to Police**	**Refer to technical support staff for action re filtering / security etc**	**Inform parents / carers**	**Removal of network / internet access rights**	**Warning**	**Further sanction**
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		✓	✓	✓	✓	✓	✓	✓	✓	✓
Unauthorised use of non-educational sites during lessons	✓	✓	✓			✓				✓
Unauthorised use of mobile phone / digital camera / other mobile device (depends on severity and frequency)	✓	✓					✓			✓
Unauthorised use of social media / messaging apps / personal email	✓	✓				✓	✓	✓		✓
Unauthorised downloading or uploading of files	✓	✓				✓	✓	✓		✓
Allowing others to access school / academy network by sharing username and passwords	✓	✓				✓	✓	✓		✓
Attempting to access or accessing the school / academy network, using another student's / pupil's account	✓	✓	✓	✓		✓	✓	✓		✓
Attempting to access or accessing the school / academy network, using the account of a member of staff		✓	✓	✓		✓	✓	✓		✓
Corrupting or destroying the data of other users		✓	✓	✓		✓	✓	✓		✓
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		✓	✓	✓	✓	✓	✓	✓		✓
Continued infringements of the above, following previous warnings or sanctions			✓	✓	✓	✓	✓	✓		✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			✓			✓	✓	✓		✓
Using proxy sites or other means to subvert the school's / academy's filtering system		✓	✓			✓	✓	✓		✓
Accidentally accessing offensive or pornographic material and failing to report the incident	✓	✓				✓			✓	✓
Deliberately accessing or trying to access offensive or pornographic material	✓	✓	✓	✓	✓	✓	✓	✓		✓
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		✓	✓			✓				✓

Appendices

Appendix 1 – Roles & Responsibilities

Appendix 2 – Education & Training

Appendix 3 - Technical – Infrastructure, Hardware & Software

Appendix 4 – Policies to Support E-Safety @ Townley

- Cyberbullying
- Social Media
- Staff Acceptable Use Policy
- Student Acceptable Use Policy
- Data Protection
- Bring Your Own Device Policy
- Data Protection

Appendix 5 – Responding to Online Safety Incidents

Appendix 6 – Resources & links

Glossary

Appendix 1 Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within Townley Grammar School.

Governors:
The Governing Body is responsible for the approval of the E-Safety Policy and for reviewing its effectiveness. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor. The role of the E-Safety Governor will include:

- regular meetings with the E-Safety Co-ordinator
- regular monitoring of e-safety incident logs
- regular monitoring of filtering / change control logs
- reporting back to the Governing Body

Headteacher & Senior Leadership Team:

- The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Co-ordinator
- The Headteacher 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 e-safety allegation being made against a member of staff. (Appendix 1 – 'Responding to Online Safety Incidents')
- The Headteacher is responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the E-Safety Co-ordinator.

E-Safety Coordinator:
The day-to-day responsibility for e-safety lies with the E-Safety Co-ordinator. The responsibilities for the E-Safety Coordinator are as follows:

- Leads the e-safety committee
- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- Provides training and advice for staff
- Liaises with school technical staff
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- Meets regularly with the governor responsible for E-Safety to discuss current issues, review incident logs and filtering
- Reports regularly to Senior Leadership Team

Network Manager & Technical staff:
The IT Services Team are responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack
- That the school meets required e-safety technical requirements outlined in the LGfL Security Policy and Acceptable Usafe Policy
- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- The filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- That they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- That the use of the network ; (internet / Virtual Learning Environment/ email) and remote access is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher and/or E-Safety Coordinator for investigation
- That monitoring systems are implemented and updated

Teaching and Support Staff
Are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current school E-Safety policy and practices
- They have read, understood and signed the Staff Acceptable Use Policy
- They report any suspected misuse or problem to the Headteacher / E-Safety Coordinator for investigation and action or sanction
- All digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems
- E-safety issues are embedded in all aspects of the curriculum and other school activities
- Students understand and follow the E-Safety and Acceptable Use Policies
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices (including student's own devices as per our BYOD policy)
- In lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use wherever possible

Safeguarding Designated Person
Should be trained in e-safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

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

All of the above are child protection issues, not technical issues, simply that the technology provides additional means for child protection issues to develop. As such these will be dealt with by trained safeguarding staff and not technicians.

E-Safety Committee
The E-Safety Committee provides a consultative group that has wide representation from the school community, with responsibility for issues regarding e-safety and the monitoring of the e-safety policy including the impact of initiatives. The group will also be responsible for regular reporting to the Governing Body.

Members of the E-safety Committee will assist the E-Safety Coordinator with:

- The review and monitoring of the school e-safety policy.
- The review and monitoring of the school filtering policy and requests for filtering changes.
- Mapping and reviewing the e-safety curricular provision – ensuring relevance, breadth and progression.
- Monitoring incident logs.
- Consulting stakeholders – including parents / carers and the students about the e-safety provision.
- Monitoring improvement actions identified through use of the 360 degree safe self review tool.

Students:

- Are responsible for using Townley Grammar's digital technology systems in accordance with the Student Acceptable Use Policy, which they will be expected to sign before being given access to school systems.
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.

Parents & Carers
Parents and carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local e-safety campaigns. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website / VLE and on-line student records
- their children's personal devices in the school

Parents and carers will be responsible for endorsing (by signature) the Student Acceptable Use Policy.

Appendix 2 Education & Training

Students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in e-safety is therefore an essential part of the school's e-safety provision. Young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-safety is a focus in all areas of the curriculum and staff reinforce e-safety messages across the curriculum. The e-safety curriculum is broad, relevant and provides progression, with opportunities for creative activities which are provided in the following ways:

- A planned e-safety curriculum is part of the Computing and PHSE offering and is regularly revisited
- Key e-safety messages are reinforced as part of a planned programme of assemblies and pastoral activities
- Students are be taught in all lessons to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information
- Students are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students should be helped to understand the need for the Student Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use wherever possible
- Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – Parents & Carers

Many parents and carers have only a limited understanding of e-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 on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters and newsletters
- The school website
- Parents evenings / sessions
- High profile events / campaigns eg Safer Internet Day, events in Enrichment Week

Education & Training – Staff

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

- A planned programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly. It is expected that some staff will identify e-safety as a training need within the performance management process.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements.
- The E-Safety Coordinator will receive regular updates through attendance at external training events and guidance documents released by relevant organisations
- This E-Safety policy and its updates will be presented to and discussed by staff as part of Continued Professional Development sessions
- The E-Safety Coordinator will provide advice / guidance / training to individuals as required.

Training – Governors

Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members of any sub committee / group involved in technology / e-safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation (eg SWGfL)
- Participation in school training / information sessions for staff or parents (this may include attendance at assemblies / lessons)

Appendix 3 Technical – Infrastructure, Hardware & Software

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

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

- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices
- All users will be provided with a username and secure password by the Network Manager – James Ayreswho will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password every (insert timeframe).
- Users are responsible for the security of their own username and password; they must not allow other users to access the systems using their log on details and must immediately report any suspiciaon or evidence that there has been a breach of security.
- The "master / administrator" passwords for the school ICT system, used by the Network Manager must also be available to the Headteacher or other nominated senior leader and kept in a secure place (eg school safe)
- The Network Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations (Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs)
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. (the school / academy will need to decide on the merits of external / internal provision of the filtering service – see appendix). There is a clear process in place to deal with requests for filtering changes (see appendix for more details)
- The school has provided enhanced / differentiated user-level filtering (allowing different filtering levels for different ages / stages and different groups of users – staff / pupils / students etc)
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement (add details of the monitoring programmes that are used)
- An appropriate system is in place (suggest to have a dedicated email address – reportit@townleygrammar.org.uk - for reporting any actual/potential e-safety incident) for users to report any actual / potential technical incident / security breach to the relevant person, as agreed)
- Appropriate security measures are in place (provide more detail) to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place (to be described) for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place (to be described) regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on school devices that may be used out of school.
- An agreed policy is in place (to be described) that allows staff to / forbids staff from downloading executable files and installing programmes on school devices.
- An agreed policy is in place (to be described) regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. (see School Personal Data Policy Template in the appendix for further detail)

Appendix 5 Policies to Support E-Safety @ Townley

Bring Your Own Device (BYOD)

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration by schools of users bringing their own technologies in order to provide a greater freedom of choice and usability. However, there are a number of e-safety considerations for BYOD that need to be reviewed prior to implementing such a policy. Use of BYOD should not introduce vulnerabilities into existing secure environments. Considerations will need to include; levels of secure access, filtering, data protection, storage and transfer of data, mobile device management systems, training, support, acceptable use, auditing and monitoring.

- The school has a set of clear expectations and responsibilities for all users
- The school adheres to the Data Protection Act Principles
- All users are provided with and accept the Acceptable Use Agreement
- All network systems are secure and access for users is differentiated
- Where possible these devices will be covered by the school's normal filtering systems, while being used on the premises
- All users will use their username and password and keep this safe
- Regular audits and monitoring of usage will take place to ensure compliance
- Any device loss, theft, change of ownership of the device will be reported as in the BYOD policy
- Any user leaving the school will follow the process outlined within the BYOD policy

Curriculum

All pupils throughout the school will have regular e-safety related activities as part of their PSHE curriculum. Key Stage 3 pupils will have discrete Digital Literacy lessons as part of their Computing curriculum, as will students opting for Computer Science and ICT at GCSE and Advanced Level.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students in the digital video/images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission

- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images
- Written permission from parents or carers will be obtained before photographs of students are published on the school website

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection

The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Responsible persons are appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data
- Transfer data using encryption and secure password protected devices

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected)

- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

Social Media - Protecting Professional Identity

All schools have a duty of care to provide a safe learning environment for pupils and staff. Schools could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

  School staff should ensure that:
- No reference should be made in social media to students / pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.