Great Torrington School

Online and Data Security Policy

Approving Committee:	**Teaching and Learning**
Review & Approval date:	**13th March 2017**
Minute Reference:	**2016-17/T&L/38**
Staff Sponsor:	**Jon Buss**
Date of next review:	**Jan 2019**
Placed on T drive:	**Jan 2017**
Placed on website:	**Yes**

Contents

Development / Monitoring / Review of this Policy

This online safety policy has been developed by the Online Safety committee made up of:

- Online Safety Officer
- Child Protection and Safeguarding Officer
- AHT – Teaching and Learning
- Staff – including Teachers, Support Staff and Technical staff
- Governor
- Feedback from Junior Leadership Team

The school will monitor the impact of the policy using:

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

Scope

This policy applies to all members of the Great Torrington School community (including staff, students, volunteers, parents / carers, visitors, community users) who have access to and are users of school / academy ICT systems, both in and out of Great Torrington 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 Great Torrington School site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online incidents covered by this policy, which may take place outside of the academy, but is linked to membership of the academy. 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.

Great Torrington 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 online behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the online roles and responsibilities of individuals and groups within Great Torrington School:

Governors

Governors are responsible for the approval of the Online and Data Security Policy and for reviewing the effectiveness of the policy. This will be carried out by the Full Governors receiving regular information about online incidents and monitoring reports. A member of the Governing Body has taken on the role of Safeguarding Governor. The role of the Online Governor will include:

- regular meetings with the Online Co-ordinator / Officer
- regular monitoring of online incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors / committee / meeting

Headteacher and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including online) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Officer
- The Headteacher and (at least) another member of the Senior Leadership Team / Senior Management Team should be aware of the procedures to be followed in the event of a serious online allegation being made

against a member of staff. (see flow chart on dealing with online safety incidents – included in a later section – “Responding to incidents of misuse”)

- The Senior Leadership Team / Senior Management Team will receive regular monitoring reports from the Online safety Co-ordinator / Officer

Online Safety Officer

- leads the online safety committee
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority / relevant body
- liaises with school technical staff and SIRO
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- meets regularly with Online Safety Governor and Child Protection and Safeguarding Officer to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of Governors
- reports regularly to Senior Leadership Team

ICT Technical staff

The ICT Support Department are responsible for ensuring:

- that Great Torrington Schools technical infrastructure is secure and is not open to misuse or malicious attack
- that Great Torrington School meets required online safety technical requirements and any DCC Online Safety Policy / Guidance that may apply
- 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 reviewed, 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 online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the network / internet / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the ICT Network for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in academy policies

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current academy online safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy (AUP) each academic year
- they report any suspected misuse or problem to the Headteacher / Child Protection and Safeguarding Officer / Online Safety Officer for investigation / action / sanction
- all digital communications with students / 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
- students understand and follow the online 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
- in lessons where internet use is pre-planned students 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
- Monitoring software (Impero) is used to control student conduct whilst using ICT. This can be used for printing, internet and application control to ensure students stay safe and on-task.

Child Protection and Safeguarding Officer

Should be trained in online 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

Online Safety committee

The Online Safety committee provides a consultative group that has wide representation from the academy community, with responsibility for issues regarding online safety and the monitoring the online safety policy including the impact of initiatives. Depending on the size or structure of the academy this committee may be part of the safeguarding group. The group will also be responsible for regular reporting to the Governing Body.

Members of the Online Safety committee will assist the Online Safety Officer with:

- the production / review / monitoring of the school online safety policy / documents.
- the production / review / monitoring of the school filtering policy and requests for filtering changes.
- mapping and reviewing the online safety curricular provision – ensuring relevance, breadth and progression with the Head of 3Rs
- monitoring network / internet / incident logs
- consulting stakeholders – including parents / carers and the students about the online safety provision
- monitoring improvement actions identified through use of the 360 degree safe self-review tool

Students

- are responsible for using the academy digital technology systems in accordance with the Student Acceptable Use Policy
- 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 online safety practice when using digital technologies out of school and realise that the academy's Online safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The academy will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local online safety campaigns / literature. Parents and carers will be encouraged to support the academy in promoting good online 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 / and on-line student / pupil records

Community Users

Community Users who access school systems as part of the wider academy provision will be expected to sign a Community User AUP before being provided with access to school systems.

Education

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 online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

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

- A planned online safety curriculum should be provided as part of ICT / 3Rs / other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- An Online Safety noticeboard will be kept relevant and up to date within the main ICT block
- Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Students should be 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 Policy 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 and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- 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 (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff 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.

Parents / carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of their 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, newsletters, web site etc.
- Parents evenings
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications

The Wider Community

The academy will provide opportunities for local community groups / members of the community to gain from the academy's online safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and online safety
- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The academy website will provide online safety information for the wider community
- Supporting community groups e.g. Early Years Settings, Childminders, youth / sports / voluntary groups to enhance their online safety provision

Staff / Volunteers

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

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and Acceptable Use Agreements.

- The Online Safety officer will receive regular updates through attendance at external training events (e.g. from SWGfL / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This Online safety policy and its updates will be presented to and discussed by staff in staff briefings / team meetings / INSET days.
- The Online Safety officer will provide advice / guidance / training to individuals as required.

Governors / Directors

Governors should take part in online safety training / awareness sessions, with particular importance for those who are members of any subcommittee / group involved in technology / online 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 (e.g. SWGfL).
- Participation in school training / information sessions for staff or parents

School Technical Security

Introduction

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The academy will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another's files (other than that allowed for monitoring purposes within the school's policies).
- access to personal data is securely controlled in line with the school's personal data policy
- logs are maintained of access by users and of their actions while users of the system
- there is effective guidance and training for users
- there are regular reviews and audits of the safety and security of school computer systems
- there is oversight from senior leaders and these have impact on policy and practice.

Responsibilities

The management of technical security will be the responsibility of the ICT Network Manager

Password Security

A safe and secure username / password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices, email and Virtual Learning Environment (VLE).

Policy Statements

- all users will have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the ICT Network Manager and will be reviewed, at least annually, by the Online Safety Committee.
- all school / academy networks and systems will be protected by secure passwords that are regularly changed.
- the "master / administrator" passwords for the school / academy systems, used by the technical staff must also be available to the ICT Network Manager and kept in a secure place e.g. school safe. Consideration should also be given to using two factor authentication for such accounts.
- passwords for new users, and replacement passwords for existing users will be allocated by ICT Support
- all users (adults and young people) will have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- users will change their passwords at regular intervals – as described in the staff and student / pupil sections below .
- the level of security required may vary for staff and student accounts and the sensitive nature of any data accessed through that account)
- requests for password changes should be authenticated by (the responsible person) to ensure that the new password can only be passed to the genuine user

Staff passwords:

- All staff users will be provided with a username and password by ICT Support
- the password should be a minimum of 8 characters long and must include three of – uppercase character, lowercase character, number, special characters
- must not include proper names or any other personal information about the user that might be known by others
- the account should be "locked out" following six successive incorrect log-on attempts
- temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on
- passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption)
- passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of school
- should be changed at least every 42 days
- should not re-used for 6 months and be significantly different from previous passwords created by the same user
- should be different for different accounts, to ensure that other systems are not put at risk if one is compromised

Student / pupil passwords

- All users will be provided with a username and password by ICT Support
- Students / pupils will be taught the importance of password security
- The complexity (i.e. minimum standards) will be set with regards to the cognitive ability of the children.

Training / Awareness

Members of staff will be made aware of the school's password policy:

- at induction
- through the school's Online Safety policy and password security policy
- through the Acceptable Use Agreement

Pupils / students will be made aware of the school's password policy:

- in lessons
- through the Acceptable Use Agreement

Audit / Monitoring / Reporting / Review

The ICT Network Manager will ensure that full records are kept of:

- User log-ons
- Security incidents related to this policy

Filtering

Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for Online Safety and acceptable use. It is important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

Responsibilities

The responsibility for the management of the school's filtering policy will be held by the ICT Network Manager. They will manage the school filtering, in line with this policy and will keep records / logs of changes and of breaches of the filtering systems.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service must:

- be logged in change control logs
- be reported to the Online Safety Group every term in the form of an audit of the change control logs

All users have a responsibility to report immediately to Online Safety Officer any infringements of the academies filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

Policy Statements

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the school. Illegal content is filtered by broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists . Filter content lists are regularly updated and internet use is logged and frequently monitored. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with school practice.

- The academy maintains and supports the managed filtering service provided by the Internet Service Provider
- The academy has also provided enhanced / differentiated user-level filtering through the use of Smoothwall allowing different filtering levels for different ages / stages and different groups of users – staff / pupils / students etc.
- In the event of the technical staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the ICT Network Manager.
- Mobile devices that access the school / academy internet connection (whether school / academy or personal devices) will be subject to the same filtering standards as other devices on the school systems
- Any filtering issues should be reported immediately to the filtering provider.
- Requests from staff for sites to be removed from the filtered list will be considered by the technical staff. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the Online Safety Committee.

Education / Training / Awareness

Students will be made aware of the importance of filtering systems through the Online Safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through:

- the Acceptable Use Agreement
- induction training
- staff meetings, briefings, Inset.

Parents will be informed of the school's filtering policy through the Acceptable Use Agreement and through Online Safety awareness sessions / newsletter etc.

Changes to the Filtering System

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to ICT Support who will decide whether to make school level changes (as above).

Monitoring

Some schools / academies supplement their filtering systems with additional monitoring systems. If this is the case, schools / academies should include information in this section, including – if they wish – details of internal or commercial systems that are in use. They should also ensure that users are informed that monitoring systems are in place.

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the School Online Safety Policy and the Acceptable Use Agreement. Monitoring will take place as follows:

- Using Smoothwall reporting
- Using Impero logging

Audit / Reporting

Logs of filtering change controls and of filtering incidents will be made available to: (schools should amend as relevant)

- Online Safety Committee
- Safeguaring Committee
- Senior Leaders
- External Filtering provider / Local Authority / Police on request

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision.

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 the academy into users bringing their own technologies in order to provide a greater freedom of choice and usability. However, there are a number of online 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. This list is not exhaustive and a BYOD policy should be in place and reference made within all relevant policies.

As such student personal devices are banned from use at GTS, this includes laptops, tablets, phones and other mobile devices. These devices should not be bought into school under any circumstance, if mobile phones are required for travel purposes they should be handed into pupil services during school hours.

Electronic Devices - Searching & Deletion

Introduction

The changing face of information technologies and ever increasing pupil / student use of these technologies has meant that the Education Acts have had to change in an attempt to keep pace. Within Part 2 of the Education Act 2011 (Discipline) there have been changes to the powers afforded to schools by statute to search pupils in order to maintain discipline and ensure safety. Schools are required to ensure they have updated policies which take these changes into account. No such policy can on its own guarantee that the school will not face legal challenge, but having a robust policy which takes account of the Act and applying it in practice will however help to provide the school with justification for what it does.

The particular changes we deal with here are the added power to search for items 'banned under the school rules' and the power to 'delete data' stored on seized electronic devices.

Items banned under the school rules are determined and publicised by the Headteacher (section 89 Education and Inspections Act 2006).

An item banned by the school rules may only be searched for under these new powers if it has been identified in the school rules as an item that can be searched for. It is therefore important that there is a school policy which sets out clearly and unambiguously the items which:

- are banned under the school rules; and
- are banned AND can be searched for by authorised school staff

The act allows authorised persons to examine data on electronic devices if they think there is a good reason to do so. In determining a 'good reason' to examine or erase the data or files the authorised staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or could break the school rules.

Following an examination, if the person has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so.

The Head Teacher must publicise the school behavior policy, in writing, to staff, parents / carers and students / pupils at least once a year. (There should therefore be clear links between the search etc. policy and the behavior policy).

Relevant legislation:

- Education Act 1996
- Education and Inspections Act 2006
- Education Act 2011 Part 2 (Discipline)
- The School Behaviour (Determination and Publicising of Measures in Academies) Regulations 2012
- Health and Safety at Work etc. Act 1974
- Obscene Publications Act 1959
- Children Act 1989
- Human Rights Act 1998
- Computer Misuse Act 1990

Responsibilities

The Headteacher is responsible for ensuring that the school policies reflect the requirements contained within the relevant legislation. The formulation of these policies may be delegated to other individuals or groups. The policies will normally be taken to Governors for approval. The Headteacher will need to authorise those staff who are allowed to carry out searches.

This policy has been written by and will be reviewed by the Online Safety Commitee

The Headteacher has authorised all staff to carry out searches for electronic devices.

The Headteacher has authorised the ICT Support Team to search electronic devices and the deletion of data / files on those devices

The Headteacher / Principal may authorise other staff members in writing in advance of any search they may undertake, subject to appropriate training.

Training / Awareness

It is essential that all staff should be made aware of and should implement the school's policy.

Members of staff should be made aware of the school's policy on "Electronic devices – searching and deletion":

- at induction
- at regular updating sessions on the school's Online Safety policy

Members of staff authorised by the Headteacher to carry out searches for and of electronic devices and to access and delete data / files from those devices should receive training that is specific and relevant to this role.

Specific training is required for those staff who may need to judge whether material that is accessed is inappropriate or illegal.

Search

The school Behaviour Policy refers to the policy regarding searches with and without consent for the wide range of items covered within the Education Act 2011 and lists those items. This policy refers only to the searching for and of electronic devices and the deletion of data / files on those devices.

Pupils/students are not allowed to bring mobile phones or other personal electronic devices to school or use them in the school.

Authorised staff (defined in the responsibilities section above) have the right to search for such electronic devices where they reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules.

- Searching with consent - Authorised staff may search with the pupil's consent for any item.
- Searching without consent - Authorised staff may only search without the pupil's consent for anything which is either 'prohibited' (as defined in Section 550AA of the Education Act 1996) or appears in the school rules as an item which is banned and may be searched for.

In carrying out the search:

- The authorised member of staff must have reasonable grounds for suspecting that a student / pupil is in possession of a prohibited item i.e. an item banned by the school rules and which can be searched for.
- The authorised member of staff should take reasonable steps to check the ownership of the mobile phone / personal electronic device before carrying out a search.
- The authorised member of staff should take care that, where possible, searches should not take place in public places e.g. an occupied classroom, which might be considered as exploiting the student / pupil being searched.
- The authorised member of staff carrying out the search must be the same gender as the student / pupil being searched; and there must be a witness (also a staff member) and, if at all possible, they too should be the same gender as the student/ pupil being searched.

There is a limited exception to this rule: Authorised staff can carry out a search of a student / pupil of the opposite gender including without a witness present, but only where you reasonably believe that there is a risk that serious harm will be caused to a person if you do not conduct the search immediately and where it is not reasonably practicable to summon another member of staff.

Extent of the search:

- The person conducting the search may not require the student/ pupil to remove any clothing other than outer clothing.
- Outer clothing means clothing that is not worn next to the skin or immediately over a garment that is being worn as underwear (outer clothing includes hats; shoes; boots; coat; blazer; jacket; gloves and scarves).
- 'Possessions' means any goods over which the student / pupil has or appears to have control – this includes desks, lockers and bags.
- A student's / pupil's possessions can only be searched in the presence of the student / pupil and another member of staff, except where there is a risk that serious harm will be caused to a person if the search is not conducted immediately and where it is not reasonably practicable to summon another member of staff.
- The power to search without consent enables a personal search, involving removal of outer clothing and searching of pockets; but not an intimate search going further than that, which only a person with more extensive powers (e.g. a police officer) can do.
- Use of Force – force cannot be used to search without consent for items banned under the school rules regardless of whether the rules say an item can be searched for.

An authorised member of staff finding an electronic device may access and examine any data or files on the device if they think there is a good reason to do so.

The examination of the data / files on the device should go only as far as is reasonably necessary to establish the facts of the incident. Any further intrusive examination of personal data may leave the school open to legal challenge.

If inappropriate material is found on the device it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police. Examples of illegal activity would include:

- child sexual abuse images (including images of one child held by another child)
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

The school should also consider their duty of care responsibility in relation to those staff who may access disturbing images or other inappropriate material whilst undertaking a search. Seeing such material can be most upsetting. There should be arrangements in place to support such staff. The school may wish to add further detail about these arrangements.

Deletion of Data

Following an examination of an electronic device, if the authorised member of staff has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so.

If inappropriate material is found on the device, it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a possible criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police.

A record should be kept of the reasons for the deletion of data / files.

Care of Confiscated Devices

School staff are reminded of the need to ensure the safe keeping of confiscated devices, to avoid the risk of compensation claims for damage / loss of such devices

Audit / Monitoring / Reporting / Review

The responsible person ICT Network Manager will ensure that full records are kept of incidents involving the searching for and of mobile phones and electronic devices and the deletion of data / files.

These records will be reviewed by Online Safety Committee at on a termly basis.

This policy will be reviewed by the head teacher and governors annually and in response to changes in guidance and evidence gained from the records.

Acceptable Use Policies

Students

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital 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.

The school will try to ensure that students / pupils will have good access to digital technologies to enhance their learning and will, in return, expect the students / pupils to agree to be responsible users.

Students AUP

1. I will only use ICT systems in school, including the internet, email, digital video, mobile technologies etc. for approved educational purposes.
2. I will not download or install software on school equipment.
3. I will only log on to the school network / online systems with my own user name and password.
4. I will not reveal my passwords to anyone and will change them regularly.
5. I will only use my school email account for approved school activities.
6. I will ensure that all ICT communications with pupils, teachers or others is responsible, sensible and appropriate.
7. I will be responsible for my behaviour when using the internet. This includes resources I access and the language I use.
8. I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher.
9. I will immediately report any unpleasant or inappropriate material, images or behaviour that makes me feel uncomfortable when using ICT.

10. I understand that the school systems are intended for educational use and I will not use them for shopping, business, social or file sharing purposes.
11. I will not give out any personal information, such as name, phone number or address. I will not arrange to meet someone unless doing so as part of a school project and it is approved by my teacher.
12. Images of pupils and / or staff will only be taken, stored and used for school purposes in line with school's policy.
13. Images of pupils and / or staff may not be distributed outside the school network without the permission of the Communications Officer.
14. I will ensure that my online activity, both in school and outside school, will not cause Great Torrington School, the staff, pupils or others distress or bring them into disrepute.
15. I will support the school's approach to online safety and not deliberately upload or add any images, videos, sounds or text that could upset or offend any member of the school community.
16. I will respect the privacy and ownership of others' work at all times.
17. I will not attempt to bypass the internet filtering system.
18. I understand that all use of the internet and other related technologies can be monitored and logged and can be made available to my teachers.
19. I understand that these rules are designed to keep me safe and that if they are not followed school sanctions will be applied and my Parent / Carer may be contacted.
20. If it can be proven that waste or malicious damage has taken place, the school reserves the right to charge an appropriate amount as recompense.
21. I will not bring a personal mobile phone, imaging or computer device into school without following current school procedures.

I have discussed this document with my Parent / Carer and I agree to follow the e-Safety rules and support the safe and responsible use of ICT throughout my entire time at Great Torrington School. I understand that if I break these rules Great Torrington School reserves the right to impose appropriate sanctions.

Parent / Carers

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of Online Safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that students will have good access to digital technologies to enhance their learning and will, in return, expect the students to agree to be responsible users. A copy of the Student Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Parent / Carers Agreement

As Parents / Carers, I / we will:

- Ensure that my child attends school regularly, on time, dressed according to the school's dress code *(see website for full details)* and is fully equipped for every lesson;
- Support the school's policies for good behaviour, including detentions / sanctions;
- Contact the school promptly about any concerns or problems that might affect my child's work or behaviour;
- Support my child in homework and other opportunities for home learning;
- Attend Parents' Evenings and discussions about my child's progress, if possible;
- Become aware of the activities surrounding the life of my child at school.

Pupils are expected to:

- Attend school regularly, on time, dressed according to the school's dress code *(see website for full details);*
- Arrive with the correct equipment, including Pupil Learning Journals;
- Follow the school's Behaviour Policy and conduct themselves in line with the school's values;
- Always attempt to give their best;
- Look after the school's resources and environment.

Great Torrington School will endeavour to:

- Enable all pupils to reach their full potential academically;
- Set, monitor and assess work within the school's Curriculum;
- Keep parents informed via regular assessment, progress checks, annual reports, Parents' Evenings, newsletters, Pupil Learning Journals and Parentmail;
- Contact parents promptly if any problem arises which affects their child's work, behaviour or attendance;
- Be available to support parents with any problems or concerns that they may have about their child's progress and behaviour;
- Set, mark and monitor homework on a regular basis.

ICT, including the internet, learning platforms, email and mobile technologies have become an important part of learning in our school. Great Torrington School expects all pupils to be safe and responsible when using any ICT. It is essential that pupils are aware of online safety and know how to stay safe when using all forms of ICT.

Pupils are expected to read and discuss the Student Acceptable Use Policy with their parent or carer and to sign and follow the terms of the agreement. *(A copy of the Student AUP is published on the school website – if you require a paper copy, please contact Reception.)* Your child will be required to sign electronically, every year, the first time they log onto the ICT system – **ICT access will not be given without their e-signature.**

- I will support the school's approach to online safety and will not deliberately upload or add any images, sounds or text that could upset or offend any member of the school community.
- I understand that if it can be proven that waste or malicious damage has taken place, the school reserves the right to charge a reasonable amount in recompense.
- The school uses CCTV for safeguarding purposes and to monitor pupil behaviour. This footage is kept for a maximum of 30 days, unless it is required as evidence.
- The school will provide sufficient printer credit to complete all required curriculum work. If any additional credit is required it can be purchased from the school at cost price.
- I understand that if the terms of the Student Acceptable Use Policy are broken the school reserves the right to apply appropriate sanctions.
- I understand that data on my child will be shared with / hosted by approved third party organisations, in order to enhance their education and provide support.
- The school reserves the right to publish students' exemplary work in order to promote the school's and pupils' achievements.

If you or your child have any concerns, or if further explanation is required on the points above, please contact your child's Tutor, ICT teacher, or the school's Senior Information Risk Officer, Mr Jon Buss.

I have discussed this document with my child and _____ *(pupil name)* agrees to follow the online safety rules, will support the safe and responsible use of ICT throughout his / her duration at Great Torrington School and will follow the school's expectations for his / her conduct.

Parent / Carer name (please print): _____

Parent / Carer signature: _____ Date: _____

Staff (and Volunteers)

New technologies have become integral to the lives of children and young people in today's society, both within schools / academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

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 / academy ICT 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 ICT in their everyday work.

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

Staff (and Volunteers) AUP

ICT (including data and voice) and the related technologies such as email, the internet and mobile devices, are an expected part of our daily working life in school.

This policy is designed to ensure that all staff members are aware of their professional responsibilities when using any form of ICT.

Access to ICT will not be provided until this policy has been signed. All staff are expected to adhere to its contents at all times.

If you have any concerns or if clarification is needed, please speak to the school's Online Safety Officer / Senior Information Risk Officer.

1. I have read, and will adhere to, the school's Online and Data Security Policy (10).
2. I will only use the school's ICT systems for professional purposes, or for uses deemed 'reasonable' by the Head Teacher or the Governing Body.
3. I will not disclose passwords provided to me by the school, or other related authorities, to anyone other than an official member of the ICT Support team.
4. I will lock my computer screen when left unattended, at all times.
5. I will keep all school issued ICT equipment physically secure at all times.
6. I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
7. I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory. Nor will I carry out any gambling, personal social networking or personal business activities using school ICT systems.
8. I will ensure that my online activity, including social networking, both in and outside school, will not bring my professional role or any member of the school community into disrepute.
9. I will not give out my personal details, such as mobile phone number and personal email address, to pupils nor will I 'friend or follow' current pupils on social networking sites, or until they reach eighteen years of age.

10. All school communications to parents / carers and pupils must use official GTS communication system(s), unless it is an emergency during offsite activities.
11. I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal / Protected / Restricted data can only be stored on the school network or on official encrypted devices.
12. Any Personal / Protected / Restricted data sent via email must be encrypted and the password sent in a separate email.
13. I will only store school data on authorised school systems / official educational sites, subject to published guidance and data impact level category.
14. I will not install any software unless I am a member of SLT / MLT and have completed the appropriate form via the ICT Support Team.
15. Images of pupils and / or staff members will only be taken, stored and used for professional purposes in line with the school's policy and only if consent has not been withdrawn by a parent, carer or staff member. Images must only be taken using school devices, unless required as evidence. All external use of images must be approved by the Communications Officer prior to use. Any trips in which a 3rd party may use images of our students must be identified to parents / carers in advance and the 'non publicity' list must be checked.
16. GTS reserves the right to use my photograph for official publicity purposes. If I wish to withdraw this I will inform the school Communications Officer in writing.
17. Personal mobile devices can be used to access school emails, however they must be pin / password protected at all times. Although supported for email access, personal mobile devices are **not** insured, therefore are brought into school at your own risk. Web access will be provided for these devices (i.e. email and internet browsing), NOT file access, however filtering restrictions will apply.
18. Personal computers are not supported by GTS and are brought into school at your own risk and are **not** insured. They must not be connected to the school network, unless via the official guest wireless access.
19. I understand that my data, use of the internet, ICT, voice and other related technology can be monitored and logged. These logs can be made available, on request, to my line manager or any member of SLT.
20. I will respect copyright, intellectual property rights and all relevant / current legislation.
21. I will support and promote the school's Online and Data Security Policy and help pupils to be safe and responsible in their use of ICT and related technologies.
22. I understand this Acceptable Use Policy forms part of the terms and conditions set out in my contract of employment.
23. Reasonable personal use of school ICT / voice systems is permitted, providing it does not conflict with your professional duties, incur the school additional cost or place any extra burden or risk to the school network.
24. Online resources required for teaching and learning must be approved by the Senior Information Risk Officer prior to use with pupils or storing GTS data.
25. Additional information regarding ICT conduct is also covered within the GTS Code of Conduct, which compliments this AUP and the Online and Data Security Policy.
26. I understand that whilst a system is provided for the backup of my data it is my responsibility to run this process as frequently as I deem appropriate. I understand that if I do not backup my data I accept the risk of data loss in the eventuality of unforeseen circumstances.
27. If I see any student data, or activity, which falls under the current prevent legislation I will immediately report this to a member of the Safeguarding Team.

User Signature

I agree to follow this Acceptable Use Policy and to support the safe and secure use of ICT throughout the school

Signature _____ Date _____

Full Name _____ (Printed)

Job title _____

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 / carers 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 e.g. 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 is 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.
- Students full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Parents / Careers permit the use of photographs of students to promote the school via the relevant Acceptable Use Policy. This permission can be revoked, in writing, via the School Communications. A log of the students effected is kept on the schools shared drive (T) and must be checked by staff prior to the publicity of any student photograph
- Student's / Pupil's work can be freely published to promote the school and its activities

Use of Biometric Systems

The school uses biometric systems for the recognition of individual children for its cashless catering system

Biometric technologies have certain advantages over other automatic identification systems as pupils do not need to remember to bring anything with them so nothing can be lost, such as a swipe card.

The school has carried out a privacy impact assessment and is confident that the use of such technologies is effective and justified in a school context.

No complete images of fingerprints are stored and the original image cannot be reconstructed from the data. That is, it is not possible for example, to recreate a pupil's fingerprint or even the image of a fingerprint from what is in effect a string of numbers.

Parents / carers are asked for permission for these biometric technologies to be used by their child

Staff

Monitoring

SLT and members of the ICT Support Team may inspect any ICT equipment owned or leased by the school at any time without prior notice.

ICT Support staff may monitor, intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to:

- confirm or obtain School business related information
- to confirm or investigate compliance with School policies, standards and procedures
- to ensure the effective operation of School ICT
- for quality control or training purposes
- to comply with a Subject Access Request under the Data Protection Act 1998
- to prevent or detect crime

ICT Support staff may, where applicable and without prior notice, access the e-mail or voice-mail account of someone who is absent in order to deal with any business-related issues retained on that account.

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act 1998, the Human Rights Act 1998 and the Regulation of Investigatory Powers Act 2000 (RIPA).

Please note that personal communications using School ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

Personal Use

Limited use of the school's ICT and telephony systems are allowed for private use providing the following criteria is met:

- Only contracted staff may use the school ICT systems for private use.
- It does not conflict with your professional duties or the expectations of GTS.
- It does not interfere with your work nor that of colleagues.
- It does not incur the school additional cost (i.e. subscriptions to email mailing list, additional internet costs etc.).
- It does not place extra burden on the network or adversely affect its performance (i.e. large downloads, storage of personal data etc.).
- It is evident to others that the use is personal and there is no risk that the name of GTS will be brought into disrepute.
- You do not use the school network to backup or store personal data (i.e. photos, videos, music libraries etc.).
- No liability will be accepted for any personal loss suffered as a result of private use of ICT.
- If you use the GTS network to access personal on-line banking facilities you do so at your own risk. Whilst GTS takes all reasonable precautions to ensure system security we are unable to guarantee its effectiveness.
- You do not download programs or software onto GTS ICT equipment for personal use.
- You adhere to all other guidance specified within this policy.

Use of the schools ICT systems is not permitted for any activities in connection with:

- Commercial enterprises, except for GTS Curriculum Enterprises.
- Playing computer games.
- Publishing web pages for private purposes.

Telephony

Telephone conversations may be recorded. However, if they are to be required as legal evidence you must notify the 3rd party that this is taking place.

CCTV

The school uses CCTV for security and safety. The only people with access to view this footage are members of SLT, MLT, Pupil Coaches, Premises and ICT Support

If copies of CCTV footage is required for evidence only Premises and ICT Support have access to this.

Public notification of CCTV use is displayed at the front of the school.

We do not use publicly accessible webcams in school.

Personal Devices

Whilst staff are allowed to bring in personal mobile devices they must be aware that they are bought in at their own risk, they are not covered on school insurance

All contact to pupils and parents / carers must be made on school devices

These devices can be connected to the school wifi, provided they are pin / password protected and do not cause an unnecessary burden on the school network.

Email

Staff should try to target emails accordingly, using the system distribution groups, to minimise the number of un-necessary messages received by staff.

Ensure you add an appropriate signature, including name, title and contact details

Enable 'out of office' notifications if you are due to be away for a period of time

Manage your mailbox, do not keep unnecessary documents or large documents in your mailbox.

Usernames and passwords should never be sent together

Equipment Security

Ensure your GTS provided ICT equipment is kept secure at all times. Lock your screen. Lock your room. Do not leave it in vulnerable positions when away from school. If your classroom could be used by others (shared room, wet weather base etc.) do not leave your laptop there, lock it in a cupboard / office.

You will not be provided with a GTS laptop / tablet without signing the appropriate issue form, see below. The device stays the property of GTS at all times and must be returned upon leaving the employ of GTS.

Ensure you backup your data on a regular basis. Use the GTS backup solution, do not backup to external / USB devices as they are not secure.

All GTS devices are encrypted, these passwords are kept centrally by ICT support and should be treated as securely as all other passwords.

Mobile Device Issue Form

Staff Name _____ Date _____

Laptop Make _____ Model _____

Serial Number _____ GTS No _____

This device has been issued to you by GTS as a tool to facilitate your work. You are bound by the following terms and conditions of use which form part of your contract of employment with GTS

1. I am responsible for this device and I will care for it in such a manner as to minimise the risk of loss or damage occurring.
2. It must be transported in a case and be stored carefully so it is not susceptible to damage. It must not be left for long periods of time inside a vehicle where temperature extremes can damage the unit or be left visible putting it at risk of theft
3. This device is insured whilst in school and at home, however it is not covered whilst in transit. Whilst in transit I must take all reasonable measures to ensure it is kept secure.
4. I may not make any personal / permanent identifying marks on the device, including adhesive labels or stickers.
5. It must not be left unattended without being secured. Acceptable methods of securing devices include locked desks, locked cabinets and locked classrooms / offices. If it is to be left anywhere outside of normal school hours it must not be visible.
6. In the case of any damage or loss due to the failure to follow relevant GTS policies, including this agreement, I understand I can be held responsible for payment of repairs, replacement or insurance excesses. GTS reserves the right to withhold payment from my salary if I fail to make the appropriate payment.
7. In the event of any loss or theft of the device I am required to obtain a police incident number immediately. I must also notify my Manager and the Network Manager for repair / replacement matters and data security immediately. In the event of damage to the device I am required to notify my Manager and the Network Manager for repair / replacement matters.
8. The device and any other accessories / components supplied must be returned to the Network Manager immediately upon termination of my employment, or at any other time as specifically directed by SLT or ICT Support.
9. Any data corruption or configuration errors caused by the installation of unauthorised or illegal software may result in the loss of data due to the need for a complete device rebuild.
10. No data which is pornographic, illegal or offensive in nature may be stored on the device.
11. I can only install software if I meet the criteria specified in the Online Safety and Data Security Policy and complete and return the appropriate form.
12. I am responsible for backing-up all data on the device. GTS cannot be held liable for lost data.

I agree to the above terms and conditions. My signature below indicates I have thoroughly read and understood the above information.

Staff Signature _____ Date _____

Software

Only ICT Support and members of MLT and SLT should install software on their GTS provided laptops. The appropriate form (see below) should be completed to ensure the compatibility and legal obligations are met.

Central records of licensed software is kept by ICT Support, this will be required in the case of an audit.

If a laptop has technical issues, and not GTS software is found on it this will not be re-installed as part of a rebuild / repair process.

Software Installation Form

To ensure the legality and compatibility of all software used at GTS any software installed by non ICT Support personnel must be detailed to the Network Manager within one working day of installation.

Only members of SLT or MLT are permitted to install software on their school laptops.

Name of software installed _____

Version of software installed _____

Software Provider / Supplier _____

Date software installed _____

Staff Name _____

Staff Signature _____

Date _____

By signing this form you are confirming that you have, to the best of your ability, checked the use of this software is legal and compatible with GTS systems.

If the software is subsequently required on a permanent basis its use will be logged and clarified by the Network Manager and all subsequent installations will be of the same version.

Breaches

A breach or suspected breach of policy by a School employee, volunteer or contractor may result in the temporary or permanent withdrawal of school ICT hardware, software or services from the offending individual.

Any policy breach is grounds for disciplinary action in accordance with the School Conduct Procedure.

Policy breaches may also lead to criminal or civil proceedings.

The Information Commissioner's Office (ICO) has powers to issue monetary penalties that came into force on 6 April 2010, allowing them to serve notices requiring organisations to pay up to £500,000 for serious breaches of the Data Protection Act.

The data protection powers of the ICO are to:

- Conduct assessments to check organisations are complying with the Act
- Serve information notices requiring organisations to provide the Information Commissioner's Office with specified information within a certain time period

- Serve enforcement notices and 'stop now' orders where there has been a breach of the Act, requiring organisations to take (or refrain from taking) specified steps in order to ensure that they comply with the law
- Prosecute those who commit criminal offences under the Act
- Conduct audits to assess whether an organisation's processing of personal data follows good practice
- Report to Parliament on data protection issues of concern

Please see the section 'Responding to Incidents of Misuse' for further detail

Online Safety Committee Terms of Reference

Purpose

To provide a consultative group that has wide representation from the academy community, with responsibility for issues regarding Online Safety and the monitoring the Online Safety policy including the impact of initiatives. This is a sub-committee of the Safeguarding Committee.

Membership

The Online Safety committee will seek to include representation from all stakeholders.
The composition of the group should include:

- SLT member/s
- Child Protection/Safeguarding officer
- Teaching staff member
- Support staff member
- Online Safety coordinator
- Governor
- Parent / Carer
- ICT Technical Support staff
- Student / pupil representation – for advice and feedback. Student / pupil voice is essential in the make-up of the Online Safety committee, but students / pupils would only be expected to take part in committee meetings where deemed relevant.
- Other people may be invited to attend the meetings at the request of the Chairperson on behalf of the committee to provide advice and assistance where necessary.
- Committee members must declare a conflict of interest if any incidents being discussed directly involve themselves or members of their families.
- Committee members must be aware that many issues discussed by this group could be of a sensitive or confidential nature
- When individual members feel uncomfortable about what is being discussed they should be allowed to leave the meeting with steps being made by the other members to allow for these sensitivities

Chairperson

The Committee should select a suitable Chairperson from within the group. Their responsibilities include:

- Scheduling meetings and notifying committee members;
- Inviting other people to attend meetings when required by the committee;
- Guiding the meeting according to the agenda and time available;
- Ensuring all discussion items end with a decision, action or definite outcome;
- Making sure that notes are taken at the meetings and that these with any action points are distributed as necessary

Duration

Meetings shall be held termly for a period of one hour. A special or extraordinary meeting may be called when and if deemed necessary.

Functions

These are to assist the Online Safety Officer with the following:

- To keep up to date with new developments in the area of Online Safety
- To (at least) annually review and develop the Online Safety policy in line with new technologies and incidents
- To monitor the delivery and impact of the Online Safety policy
- To monitor the log of reported Online Safety incidents (anonymous) to inform future areas of teaching / learning / training.
- To co-ordinate consultation with the whole school community to ensure stakeholders are up to date with information, training and/or developments in the area of Online Safety. This could be carried out through:
    - Staff meetings
    - Student / pupil forums (for advice and feedback)
    - Governors meetings
    - Surveys/questionnaires for students / pupils, parents / carers and staff
    - Parents evenings
    - Website/VLE/Newsletters
    - Online Safety events
    - Internet Safety Day (annually held on the second Tuesday in February)
    - Other methods
- To ensure that monitoring is carried out of Internet sites used across the school
- To monitor filtering / change control logs (e.g. requests for blocking / unblocking sites).
- To monitor the safe use of data across the [school]
- To monitor incidents involving cyberbullying for staff and pupils

Personal Data Handling

Introduction

Schools and their employees should do everything within their power to ensure the safety and security of any material of a personal or sensitive nature

It is the responsibility of all members of the school community to take care when handling, using or transferring personal data that it cannot be accessed by anyone who does not:

- have permission to access that data, and/or
- need to have access to that data.

Data breaches can have serious effects on individuals and / or institutions concerned, can bring the school into disrepute and may well result in disciplinary action, criminal prosecution and fines imposed by the Information Commissioners Office for the school and the individuals involved. Particularly, all transfer of data is subject to risk of loss or contamination.

Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the legal requirements contained in relevant data protection legislation and relevant regulations and guidance.

Policy Statements

The school 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”.

Personal Data

The school and individuals will have access to a wide range of personal information and data. The data may be held in a digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

- Personal information about members of the school community – including *students*, members of staff and parents / carers e.g. names, addresses, contact details, legal guardianship contact details, health records, disciplinary records
- Curricular / academic data e.g. class lists, pupil / student progress records, reports, references
- Professional records e.g. employment history, taxation and national insurance records, appraisal records and references
- Any other information that might be disclosed by parents / carers or by other agencies working with families or staff members

Responsibilities

The school's Senior Information Risk Officer (SIRO) is Jon Buss. This person will keep up to date with current legislation and guidance and will:

- determine and take responsibility for the school's information risk policy and risk assessment
- appoint the Information Asset Owners (IAOs)

The school will identify Information Asset Owners (IAOs) for the various types of data being held (e.g. pupil / student information / staff information / assessment data etc.) The IAOs will manage and address risks to the information and will understand:

- what information is held, for how long and for what purpose,
- how information has been amended or added to over time, and
- who has access to protected data and why.

Everyone in the school has the responsibility of handling protected or sensitive data in a safe and secure manner.

Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor.

Registration

The school is registered as a Data Controller on the Data Protection Register held by the Information Commissioner. http://www.ico.gov.uk/what_we_cover/register_of_data_controllers.aspx

Training & awareness

All staff will receive data handling awareness / data protection training and will be made aware of their responsibilities, as described in this policy through:

- Induction training for new staff
- Staff meetings / briefings / Inset
- Day to day support and guidance from Information Asset Owners

Risk Assessments

Information risk assessments will be carried out by Information Asset Owners to establish the security measures already in place and whether they are the most appropriate and cost effective. The risk assessment will involve:

- Recognising the risks that are present
- Judging the level of the risks (both the likelihood and consequences); and
- Prioritising the risks.

Risk assessments are an ongoing process and should result in the completion of an Information Risk Actions Form (example below):

Risk ID	Information Asset affected	Information Asset Owner	Protective Marking (Impact Level)	Likelihood	Overall risk level (low, medium, high)	Action(s) to minimise risk

Impact Levels and protective marking

Following incidents involving loss of data, the Government recommends that the Protective Marking Scheme should be used to indicate the sensitivity of data. The Protective Marking Scheme is mapped to Impact Levels as follows:

Government Protective Marking Scheme label	Impact Level (IL)	Applies to schools?
NOT PROTECTIVELY MARKED	0	Will apply in schools
PROTECT	1 or 2	
RESTRICTED	3	
CONFIDENTIAL	4	Will not apply in schools
HIGHLY CONFIDENTIAL	5	
TOP SECRET	6	

The school will ensure that all school staff, independent contractors working for it, and delivery partners, comply with restrictions applying to the access to, handling and storage of data classified as Protect, Restricted or higher. Unmarked material is considered 'unclassified'. The term 'UNCLASSIFIED' or 'NON' or 'NOT PROTECTIVELY MARKED' may be used to indicate positively that a protective marking is not needed.

All documents (manual or digital) that contain protected or restricted data will be labelled clearly with the Impact Level shown in the header and the Release and Destruction classification in the footer.

Users must be aware that when data is aggregated the subsequent impact level may be higher than the individual impact levels of the original data. Combining more and more individual data elements together in a report or data view increases the impact of a breach. A breach that puts students / pupils at serious risk of harm will have a higher impact than a risk that puts them at low risk of harm. Long-term significant damage to anyone's reputation has a higher impact than damage that might cause short-term embarrassment.

Release and destruction markings should be shown in the footer e.g. "Securely delete or shred this information when you have finished using it".

Secure Storage of and access to data

The school will ensure that ICT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.

All users will use strong passwords which must be changed regularly. User passwords must never be shared.

Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.

All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

Personal data can only be stored on school equipment. Private equipment (i.e. owned by the users) must not be used for the storage of personal data.

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

- the data must be encrypted and password protected,
- the device must 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.

The academy has clear policy and procedures for the backing up, accessing and restoring all data held on school systems, including off-site backups.

The academy has clear policy and procedures for the use of "Cloud Based Storage Systems" (for example dropbox, google apps and google docs) and is aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act. The school will ensure that it is satisfied with controls put in place by remote / cloud based data services providers to protect the data.

As a Data Controller, the academy is responsible for the security of any data passed to a "third party". Data Protection clauses will be included in all contracts where data is likely to be passed to a third party.

All paper based Protected and Restricted (or higher) material must be held in lockable storage, whether on or off site.

The academy recognises that under Section 7 of the DPA data subjects have a number of rights in connection with their personal data, the main one being the right of access. Procedures are in place to deal with Subject Access Requests i.e. a written request to see all or a part of the personal data held by the data controller in connection with the data subject. Data subjects have the right to know: if the data controller holds personal data about them; a description of that data; the purpose for which the data is processed; the sources of that data; to whom the data may be disclosed; and a copy of all the personal data that is held about them. Under certain circumstances the data subject can also exercise rights in connection with the rectification; blocking; erasure and destruction of data.

Secure transfer of data and access out of school

The school recognises that personal data may be accessed by users out of school, or transferred to the LA or other agencies. In these circumstances:

- Users may not remove or copy sensitive or restricted or protected personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of school
- When restricted or protected personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform;
- If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software; and
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority (if relevant) in this event.

Disposal of data

The school will comply with the requirements for the safe destruction of personal data when it is no longer required.

The disposal of personal data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, in accordance with government guidance, and other media must be shredded, incinerated or otherwise disintegrated for data.

Audit Logging / Reporting / Incident Handling

It is good practice, as recommended in the "Data Handling Procedures in Government" document that the activities of data users, in respect of electronically held personal data, will be logged and these logs will be monitored by responsible individuals.

The audit logs will be kept to provide evidence of accidental or deliberate data security breaches – including loss of protected data or breaches of an acceptable use policy.

The school has a policy for reporting, managing and recovering from information risk incidents, which establishes:

- a "responsible person" for each incident;
- a communications plan, including escalation procedures;
- and results in a plan of action for rapid resolution; and
- a plan of action of non-recurrence and further awareness raising.

All significant data protection incidents must be reported through the SIRO to the Information Commissioner's Office based upon the local incident handling policy and communication plan.

Privacy Notice

In order to comply with the fair processing requirements of the DPA, the school will inform parents / carers of all students of the data they collect, process and hold on the pupils / students, the purposes for which the data is held and the third parties (eg LA, DfE, etc) to whom it may be passed. This privacy notice will be passed to parents / carers through the website and the newsletter.

PRIVACY NOTICE
for
Great Torrington School

Privacy Notice - Data Protection Act 1998

We Great Torrington School are a data controller for the purposes of the Data Protection Act. We collect information from you and may receive information about you from your previous school and the Learning Records Service. We hold this personal data and use it to:

- Support your teaching and learning;
- Monitor and report on your progress;
- Provide appropriate pastoral care, and
- Assess how well your school is doing.

This information includes your contact details, national curriculum assessment results, attendance information and personal characteristics such as your ethnic group, any special educational needs and relevant medical information. If you are enrolling for post 14 qualifications we will be provided with your unique learner number (ULN) by the Learning Records Service and may also obtain from them details of any learning or qualifications you have undertaken.

Once you are aged 13 or over, we are required by law to pass on certain information to providers of youth support services in your area. This is the local authority support service for young people aged 13 to 19 in England. We must provide both your and your parent's/s' name(s) and address, and any further information relevant to the support services' role. However, if you are over 16, you (or your parent(s)) can ask that no information beyond names, address and your date of birth be passed to the support service. Please inform (Insert name of School Administrator) if you wish to opt-out of this arrangement. For more information about young peoples' services, please go to the Directgov Young People page at www.direct.gov.uk/en/YoungPeople/index.htm or the LA website shown above.

We will not give information about you to anyone outside the school without your consent unless the law and our rules allow us to.

We are required by law to pass some information about you to the Local Authority and the Department for

Education (DfE)

We are required by law to pass some information about you to the Department for Education (DfE) and, in turn, this will be available for the use(s) of the Local Authority.

If you want to see a copy of the information about you that we hold and/or share, please contact the school Business Manager

If you require more information about how the Local Authority (LA) and/or DfE store and use your information, then please go to the following websites:

http://www.devon.gov.uk/data_protection.htm
http://www.education.gov.uk/researchandstatistics/datatdatam/b00212337/datause

If you are unable to access these websites we can send you a copy of this information. Please contact the LA or DfE as follows:

Information Governance Team, Room 120
County Hall, Exeter
EX2 4QD
Email: accesstoinformation – mailbox@devon.gov.uk
Telephone: 01392 383881

Public Communications Unit, Department for Education
Sanctuary Buildings, Great Smith Street, London
SW1P 3BT
Website: www.education.gov.uk
email: http://www.education.gov.uk/help/contactus
Telephone: 0370 000 2288

Disposal of ICT Equipment

All redundant ICT equipment will be disposed of through an authorised agency. This should include a written receipt for the item(s) including an acceptance of responsibility for the destruction of any personal data.

All redundant ICT equipment that may have held personal data will have the storage media over written multiple times to ensure that the data is irretrievably destroyed. Alternatively if the storage media has failed it will be physically destroyed. We will only use authorised companies who supply a written guarantee that this will happen.

Disposal of any ICT equipment will conform to:

- The Waste Electrical and Electronic Equipment Regulations 2006.
- The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007.
- Electricity at Work Regulations 1989.

The school will maintain a comprehensive inventory of all its ICT equipment including a record of disposal.

The school's disposal record will include:

- Date item disposed of
- Authorisation for disposal, including:
    - Verification of software licensing
    - Any personal data likely to be held on the storage media. If personal data is likely to be held the storage media will be over written multiple times to ensure the data is irretrievably destroyed
- How it was disposed of e.g. waste, gift, sale etc.
- Name of the person and / or organisation who received the disposed item

Further information is available via Waste Electrical and Electronic Equipment (WEEE) Regulations and the Environment Agency web site

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff & other adults			Students				
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	X			X				
Use of mobile phones in lessons				X				
Use of mobile phones in social time	X			X				
Taking photos on personal mobile phones / cameras				X				
Use of other personal mobile devices e.g. tablets, laptops	X			X				
Use of personal email addresses in school, or on school network		X		X				
Use of school email for personal emails		X		X				
Use of messaging apps				X				
Use of social media		X		X				
Use of blogs		X					X	

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

- The official academy email service may be regarded as safe and secure and is monitored. Users should be aware that email communications can be monitored. Staff and students should therefore use only the school / academy email service to communicate with others when in school, or on school / academy systems (e.g. by remote access).
- Users must immediately report, to the nominated person – in accordance with the academy policy, 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) academy systems. Personal email addresses, text messaging or social media must not be used for these communications.
- All students and staff are provided with individual email accounts. Only your own account should be used for communication, never anothers.
- Students should be taught about online 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 / academy website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies and local authorities 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 academy or local authority 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, 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 academy or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

The academy's use of social media for professional purposes will be checked regularly by the SIRO and online safety committee to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

Unsuitable / inappropriate 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:

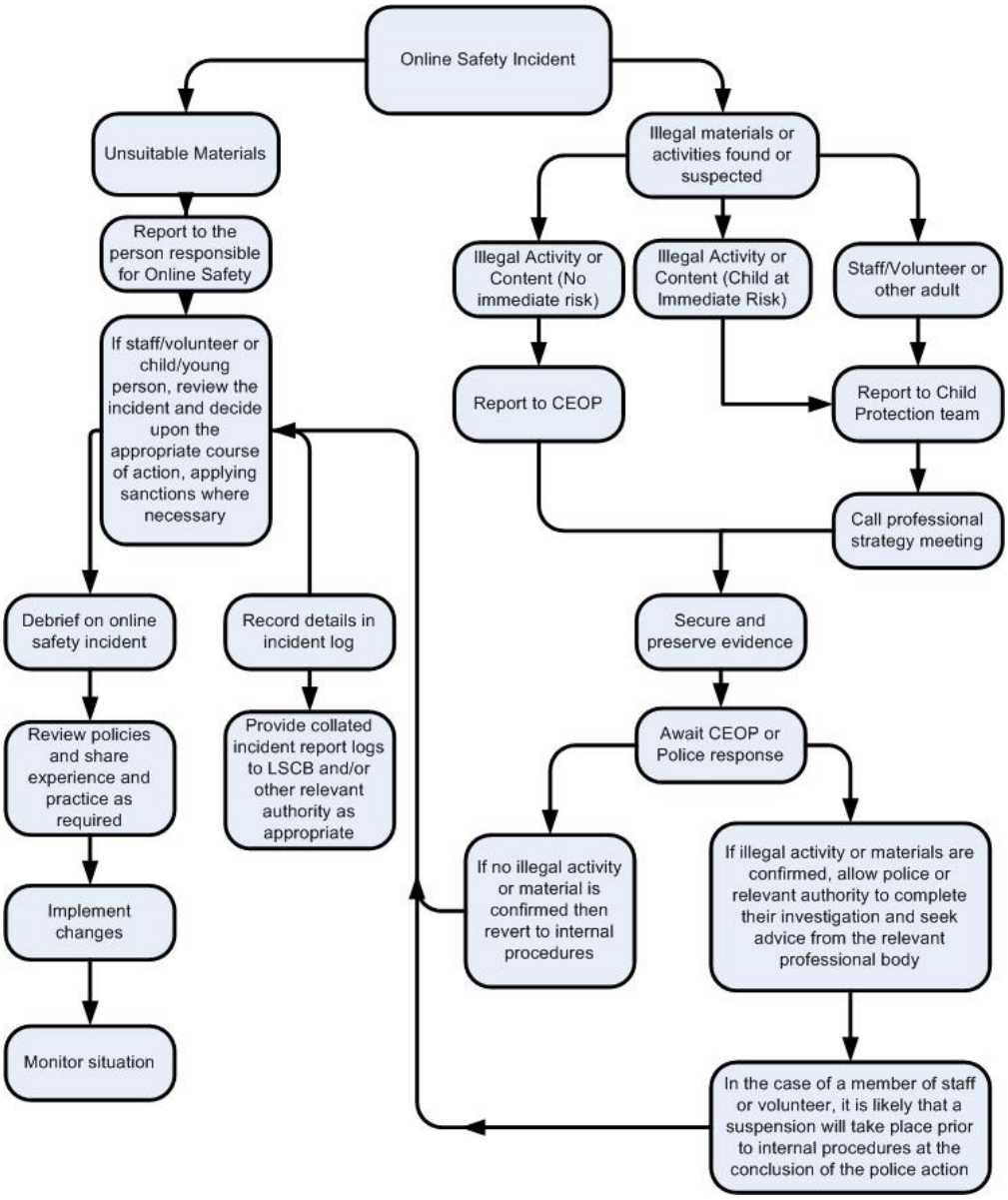
		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational) – unless with agreement of the teacher					X	
On-line gaming (non educational)					X	
On-line gambling					X	
On-line shopping / commerce					X	
File sharing					X	
Use of social media					X	
Use of messaging apps					X	
Use of video broadcasting eg Youtube – (other than KS4 only with prior arrangement)					X	

Responding to incidents of 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).

Illegal Incidents

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.



Other Incidents

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

Any actual, or attempted, security breach, loss of equipment or unauthorised misuse of ICT must be reported to the school SIRO immediately.

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

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

Reporting Log

GTS Online Safety Incident Log

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

Actions & Sanctions

It is more likely that the academy 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 behaviour / disciplinary procedures following the published Conduct Policy, Behaviour Policy and Prevent policy.

Legislation

Schools should be aware of the legislative framework under which this Online Safety Policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an e safety issue or situation.

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data Protection Act 1998

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. youtube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006

Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data.

The Protection of Freedoms Act 2012

Requires schools to seek permission from a parent / carer to use Biometric systems

The School Information Regulations 2012

Requires schools to publish certain information on its website:

http://www.education.gov.uk/schools/toolsandinitiatives/cuttingburdens/b0075738/reducing-bureaucracy/requirements/changestoschoolinformationregulations

Glossary of terms

AUP	Acceptable Use Policy – see templates earlier in this document
CEOP	Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CPC	Child Protection Committee
CPD	Continuous Professional Development
CYPS	Children and Young Peoples Services (in Local Authorities)
FOSI	Family Online Safety Institute
EA	Education Authority
ES	Education Scotland
HWB	Health and Wellbeing
ICO	Information Commissioners Office
ICT	Information and Communications Technology
ICTMark	Quality standard for schools provided by NAACE
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
LA	Local Authority
LAN	Local Area Network
MIS	Management Information System
NEN	National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
SWGfL	South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW
TUK	Think U Know – educational Online Safety programmes for schools, young people and parents.
WAP	Wireless Application Protocol