Online Safety Policy

Version control

The table below shows the history of the document and the changes made at each version:

Version	Date	Summary of changes
3.0	June 2016	
3.1	Jan 2020	Reviewed and amended References to Data Protection Act 1998 amended to Data Protection Act 2018 (throughout the document) **Page 13** clarifying GAfE – Google Apps for Education **Page 19** – clarification of encryption of personal devices **Page 28** – clarification of the term 'volunteer' in the context of the school **Page 28** – added additional popular social media sites – Instagram and snapchat **Page 28** – Inserted confirmation of Cotham school's list of official sites **Page 29** – deleted '. Instead, if they receive such requests from children or students who are not family members. Not needed as part of the policy text. Page 29 - Scope - clarification added regarding volunteers and contractors **Page 42** – Responding to incidents of misuse - staff – Incidents - 'Corrupting or destroying the data of other users or causing deliberate damage to hardware or software' Suspension – added 'potentially' and Disciplinary action – added 'potentially' **Page 42** – Responding to incidents of misuse – staff – incidents – 'Actions which could compromise the staff member's professional standing' – Disciplinary action – added 'potentially' **Page 42** – Responding to incidents of misuse – staff – incidents – 'Actions which could bring the school into disrepute or breach the integrity of the ethos of the school' – Disciplinary action – added 'potentially' **Page 47** – Clarification of the term volunteer in the context of the school **Page 52** – Addition of correct Photograph/Video Parental Consent form now used post GDPR
3.2	June 2020	**All references of e safety changed to Online safety** **Changed all references to Child Protection officer or Designated person for Child Protection to Designated Safeguarding Lead or DSL** **Page 3-** deletedSchools are expected to evaluate their level of e-safety in the Ofsted Self Evaluation Form (SEF) and will be subject to an increased level of scrutiny by Ofsted Inspectors during school inspections. **Page 7-8** reference to 2019 *Teaching online safety in schools* and reference to challenges and opportunities raised by the Covid-19 pandemic for e safety **Page 10-** Under DSL added 'Provides information for parents/ carers and students around online afety'

		Page 19- Updated Teaching E Safety in the curriculum to include information from 2019 *Teaching Online Safety in Schools* removed flow chart referencing historic approach to tackling cyber bullying **Page 54**- updated with current consent form

Approved by Governors: 4 October 2016 Policy Author: TW

Introduction

National guidance suggests that it is essential for schools to take a leading role in online safety.

In “Safeguarding Children in a Digital World” suggests:
“That schools support parents in understanding the issues and risks associated with children’s use of digital technologies. Furthermore, recommends that all schools have acceptable use policies, and ensure that parents are aware of the procedures for online safety within the school. Recognising the growing trend for home-school links and extended school activities, recommends that schools take an active role in providing information and guidance for parents on promoting online safety messages in home use of ICT, too.”

The Byron Review “Safer Children in a Digital World” stressed the role of schools:
“One of the strongest messages I have received during my Review was about the role that schools and other services for children and families have to play in equipping children and their parents to stay safe online. To empower children and raise the skills of parents, I make recommendations to Government in the following areas: delivering online safety through the curriculum, providing teachers and the wider children’s workforce with the skills and knowledge they need, reaching children and families through Extended Schools and taking steps to ensure that Ofsted holds the system to account on the quality of delivery in this area.”

The development and expansion of the use of ICT, and particularly of the internet, has transformed learning in schools in recent years. Children and young people will need to develop high level ICT skills, not only to maximise their potential use as a learning tool, but also to prepare themselves as lifelong learners and for future employment. There is a large body of evidence that recognises the benefits that ICT can bring to teaching and learning. Schools have made a significant investment both financially and physically to ensure these technologies are available to all learners. The benefits are perceived to “outweigh the risks.” However, schools must, through their online safety policy, ensure that they meet their statutory obligations to ensure that children and young people are safe and are protected from potential harm, both within and outside school.

The 2019 guidance around Teaching Online Safety in Schools outlines how schools can ensure their pupils understand how to stay safe online as part of existing curriculum requirements. This policy and the curriculum more broadly has been reviewed in line with these requirements.

The Covid-19 pandemic has thrown to light the importance of effective online provision but has also raised the risks of potential online harm. With teaching and communication primarily taking place online the school has reviewed its safeguarding and training procedures to ensure that all stakeholders have adequate information about online safety and that we can respond swiftly and appropriately where there are concerns.

1. Scope of the Policy

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

The Education and Inspections Act 2006 empowers Head Teachers, to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

Cotham 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 safety behaviour that take place out of school.

2. Roles and Responsibilities

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

Head Teacher and Senior Leadership Team (SLT):

- The Head Teacher is responsible for ensuring the safety (including online safety) of members of the school community, although the day to day responsibility for online safety is delegated to the Designated Safeguarding Lead.
- The Head Teacher / SLT are responsible for ensuring that the Designated Safeguarding Lead and other relevant staff receive suitable CPD to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Head Teacher / SLT will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Head Teacher and at least one other member of the SLT are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

Designated Safeguarding Lead:

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
- Provides information for parents/ carers and students around online safety
- Liaises with IT Services Team
- Receives reports of online safety incidents and ensures a log of incidents to inform online safety is kept by the IT Services Team
- Reports regularly to the SLT

Is trained in online safety issues and is aware of the potential for serious child protection 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

IT Services Team

IT Services Team are responsible for ensuring:

- That the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- That Cotham School meets the online safety technical requirements outlined in this document.
- That users may only access the school's networks through a properly enforced password protection policy.
- Bristol City Council (as the Internet Service Provider) is informed of issues relating to filtering.
- The school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- That they keep up to date with 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 / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Designated Safeguarding Lead for investigation / action / sanction.
- That monitoring software / systems are implemented and updated as agreed.

Teaching and Associate Staff

Are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current school online safety policy and practices
- They have read, understood and signed the school Staff Acceptable Use Agreement
- They report any suspected misuse or problem to the Designated Safeguarding Lead /Head Teacher / SLT / IT Services Manager
- Digital communications with students should be on a professional level and only carried out using official Cotham School systems
- Online safety issues are embedded in all aspects of the curriculum and other Cotham School activities
- Students understand and follow Cotham School online safety and acceptable use policy
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor ICT activity in lessons, extra curricular and extended school activities
- They are aware of online safety issues related to the use of mobile devices and that they monitor their use and implement current Cotham School 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.

Students:

- are responsible for using Cotham School ICT systems in accordance with the Student Acceptable Use Agreement, which they will be expected to accept electronically at first login before being given access to ICT systems.
- have a good understanding of research skills and the need to avoid plagiarism and

uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Will be expected to know and understand Cotham School policies on the use of mobile devices. They should also know and understand school 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 Online Safety Policy covers their actions out of school, if related to their membership of the school.

Parents/Carers

Parents and carers are responsible for:

- Endorsing the Student Acceptable Use Policy.
- Accessing the school website and other school systems in accordance with the relevant school Acceptable Use Policy.

- Supporting students to access and engage with remote learning where appropriate.

3. Policy Statements

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 staff to recognise and avoid online safety risks and build their resilience.

Online Safety education is provided in the following ways:

- A planned online safety programme is provided as part of Computing/ICT and other lessons. This provision is regularly revisited – this covers both the use of ICT and new technologies in school and outside school.
- Key online safety messages are reinforced as part of a planned programme of assemblies and tutorial / pastoral activities.
- Students are taught in all lessons to be critically aware of the materials / content they access on-line and are guided to validate the accuracy of information. Students are helped to understand the need to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Students are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet. Acceptable use of ICT systems / internet policies will be displayed at login once every two weeks.
- Staff should act as good role models in their use of ICT, the internet and mobile devices

Education – Parents/Carers

Parents and carers have a wide range of understanding of online safety risks and issues, and they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line experiences. Parents may either underestimate or not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it.

Cotham School will therefore seek to provide information and awareness to parents and carers through:

- Workshops, Letters, newsletters, website, Parents' evenings, including reference to external organisations where further information can be obtained.

Education and Training – Governors and Staff

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.
- An audit of the online safety training needs of all staff will be carried out regularly. It is expected that some staff will identify online safety as a training need within the

approved process.

- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand this policy and Acceptable Use Policies
- This Online Safety policy and its updates will be presented to and discussed by staff in team meetings.
- Governors should take part in online safety training.

4. Password Security

Introduction

Cotham School will be responsible for ensuring that the 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, without permission (or as 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

Responsibilities

The management of the password security policy will be the responsibility of the IT Services Team.

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.

Training / Awareness

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

- through the school's Online Safety policy and password security policy.
- through the Acceptable Use Agreement.
- through the IT induction programme which is led by the IT Services Manager.

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

- in Computing lessons and/or online safety assemblies.
- through the Acceptable Use Agreement.

All users will have clearly defined access rights to Cotham School ICT systems. Details of the access rights available to groups of users will be recorded by the IT Services Team and will be reviewed, at least annually, by the Online Safety Working Group. All users will be provided with a username and password by the IT Services Team who will keep an up to date record of users and their usernames.

- The password should be a minimum of 8 characters long
- Authentication process should protect against brute force attacks
- Passwords shall not be displayed on screen
- Authentication shall be encrypted
- Requests for password changes should only be managed by sanctioned staff
- Only IT Services Team will have access to change staff passwords
- All administrative users will use unique administrative accounts to support

accountability

5. 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. It is therefore 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.

The Internet is monitored and filtered using Netsweeper which is provided by our ISP (Bristol City Council). All Windows and Mac IT suites have NetSupport School installed, which allows the classroom teacher to layer on additional white and black listings, and suspend internet access for individual students during the lesson.

Responsibilities

The responsibility for the management of the filtering policy will be held by the IT Services Manager. They will manage the school filtering, in line with this policy and will ensure logs of changes and breaches of the filtering systems are kept by the IT Services Team.

All users have a responsibility to report immediately to the IT Services Team (students can refer to staff who can forward the information to the IT Services Team) any infringements of the school's 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.

Education / Training / Awareness

Students will be made aware of the importance of filtering systems through the online safety education programme (eg In ICT lessons and through assemblies). 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:

- signing the AUP
- induction training
- Inset

Parents will be informed of the school's filtering policy through the Acceptable Use Guidance and through occasional online safety awareness publications etc.

Changes to the Filtering System

Staff users may request changes to the filtering with a Helpdesk request to the IT Services

Team.

There should be strong educational reasons for changes and these changes may be for specific groups of users. The changes may be rejected for technical reasons due to the limitations of filtering systems as well as judgements about the appropriateness of materials.

All changes (and requests for change) must be logged by the technical support staff.

Monitoring

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. The majority of Google Apps for Education (GAfE) interactions are logged and can be searched using the GAfE management tool.

Audit / Reporting

Logs of filtering change controls and of filtering incidents will be made available to:

- The Head Teacher
- IT Steering Group
- Governors 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.

Infrastructure and Equipment for filtering and monitoring

Cotham School will be responsible for ensuring that the infrastructure and network is as safe and secure as is reasonably possible.

- There will be regular reviews and audits of the safety and security of Cotham School ICT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the IT Services Team and will be reviewed, at least annually, by the I.T Manager
- All users will be provided with a username and password by the IT Services Team who will keep an up to date record of users and their usernames.
- Requests from staff for sites to be removed from the filtered list will be considered by the IT Services Manager
- The IT Services Team regularly sample, record the activity and documents of users on the school ICT systems and users are made aware of this in the Acceptable Use Agreement
- Remote management tools will be used by staff to control workstations and view users' activity
- Any online safety incidents should be reported to the IT Services Team by logging a ticket on the IT Services Helpdesk
- Appropriate security measures are in place to protect the servers, firewalls, routers,

wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data
- The downloading of executable files by users is not allowed
- Staff are unable to install programmes on school workstations / portable devices
- The infrastructure and individual workstations are protected by up to date antivirus software

Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

6. Online Safety in the Curriculum

It is important to teach pupils about the underpinning knowledge and behaviours that can help pupils to navigate the online world safely and confidently regardless of the device, platform or app. However, schools also need an understanding of the risks that exist online so they can tailor their teaching and support to the specific needs of their pupils.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages in the use of ICT across the curriculum.

- 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, e.g. using search engines, 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, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the site is unblocked. The IT Services Manager (and other relevant person) can action this request if it is appropriate to do so. Any request to do so, should be auditable, with clear reasons for the need.
- 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.

- Vulnerable pupils may need additional or more personalised approaches to understanding the risks and how to keep themselves safe online.

7. Use of digital Photographic 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 and students need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees.

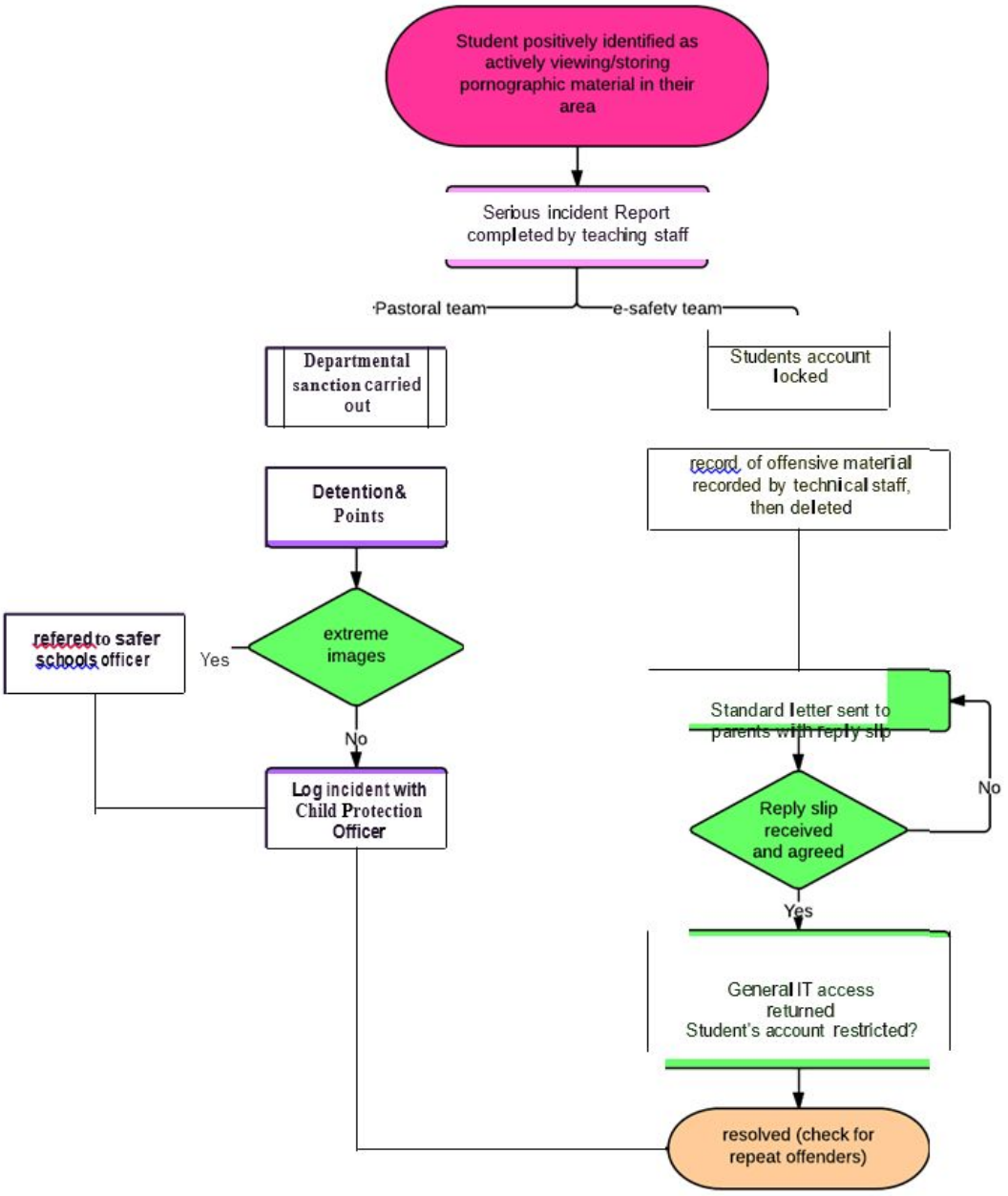
Cotham School will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- 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.
- Staff 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. These images should only be taken on school equipment, the personal equipment owned by staff should not be used for such purposes (unless prearranged and logged with the Designated Safeguarding Lead).
- 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 the schools data protection policy and good practice guidance on the use of such images
- Students' names will not be used anywhere on a website or blog, particularly in association with photographs unless written consent has been provided so that the school may do so
- Consent from parents or carers will be obtained before photographs of students are published on the school website
- Students' work can only be published with the permission of the student and parent/carers

8. Cyber Bullying

Cyber bullying is dealt with the same severity as other forms of bullying. Please reference the anti- bullying policy for more information.

Inappropriate content



9. Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 which states that personal data must be:

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

Staff must ensure that they:

- At all times take care to ensure the safekeeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer personal data using encryption and secure password protected devices.
- When personal data (other than academic or curricular data) is stored on any portable computer system, USB stick or any other removable media: the data must be encrypted and password protected
- only transport data on encrypted USB sticks. Encryption is enforced for all staff on USB sticks and it is not possible to write to a USB stick until encryption has taken place.
- When using cloud based storage, it is also necessary that staff ensure that only appropriate and authorised parties have shared access

10. Staff Protocol for IT Systems

The School's electronic communications systems and equipment are intended to promote effective communication and working practices throughout the School and are critical to the success of our provision of excellent service. The School will use ICT skills to enhance teaching and learning, to improve students' results and help students to gain skills that they will be required to use when they leave school.

This policy does not form part of any employee's terms and conditions of employment and is not intended to have contractual effect. It is provided for guidance to all members of Staff at the School who are required to familiarise themselves and comply with its contents. The School reserves the right to amend its content at any time.

This policy outlines the standards that the School requires all users of these systems to observe, the circumstances in which the School will monitor use of these systems and the action the School will take in respect of any breaches of these standards.

The use by Staff and monitoring by the School of its electronic communications systems is likely to involve the processing of personal data and is therefore regulated by the Data Protection Act 2018 together with the Employment Practices Data Protection Code issued by the Information Commissioner.

Staff are referred to the School's Data Protection Policy for further information. The School is also required to comply with the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 and the principles of the European Convention on Human Rights incorporated into U.K. law by the Human Rights Act 1998.

All members of Staff are required to comply with the provisions set out in this policy at all times to protect the School's electronic systems from unauthorised access or harm. Breach of this policy will be regarded as a disciplinary offence and dealt with under the School's disciplinary procedure and in serious cases may be treated as gross misconduct leading to summary dismissal.

The School has the right to monitor all aspects of its systems, including data which is stored under the School's computer systems in compliance with the Data Protection Act 2018.

This policy mainly deals with the use (or misuse) of computer equipment, email, internet connection, telephones, smart phones and voicemail, but it applies equally to the use of fax machines, copiers, scanners, and the like.

Equipment Security and passwords

All members of Staff are responsible for the security of the equipment allocated to or used by them and must not allow it to be used by anyone other than in accordance with this policy. Staff are encouraged to select a password that cannot be easily broken and which contains at least 8 characters including both numbers, letters and changes in case. Passwords must be kept confidential and must not be made available to anyone else. With the authorisation of the Senior Leadership Group, access to staff user areas can be obtained. Any member of Staff who discloses his or her password to another employee in the absence of express

authorisation will be liable to disciplinary action under the School's Disciplinary Policy and Procedure. Any member of Staff who logs on to a computer using another member of Staff's password will be liable to disciplinary action up to and including summary dismissal for gross misconduct.

Staff are responsible for the security of their terminals. Staff are required to log off or lock their computer when they are leaving the terminal unattended or when leaving the office to prevent unauthorised users accessing the system in their absence. The Senior Leadership Group and or IT Services Manager may do spot checks from time to time to ensure compliance with this requirement.

Staff should be aware that if they fail to log off and leave their terminals unattended they may be held responsible for another user's activities on their terminal in breach of this policy, the School's Data Protection Policy and/or the requirement for confidentiality in respect of certain information.

Logging off prevents another member of Staff accessing the system in the user's absence and may help demonstrate in the event of a breach in the user's absence that he or she was not the party responsible.

On the termination of employment for any reason, the School reserves the right to require employees to hand over all School data held in computer usable format.

Members of Staff who have been issued with a laptop, smart phones or tablets must ensure that it is kept secure at all times, especially when travelling. Passwords must be used to secure access to data kept on such equipment to ensure that confidential data is protected in the event that the machine is lost or stolen. Staff should also observe basic safety rules when using such equipment e.g. ensuring that they do not use or display such equipment in isolated or dangerous areas. Staff should also be fully aware that if using equipment on public transport documents can be easily read by other passengers.

Systems Use and Data Security

Members of Staff should not delete, destroy or modify any of the School's existing systems, programs, information or data which could have the effect of harming or exposing to risk or harm the School's, its Staff, students, or any other party.

The School monitors all emails passing through its systems for viruses. Staff should be cautious when opening emails from unknown external sources or where for any reason an email appears suspicious (such as ending in '.exe'). The IT Services Manager should be informed immediately if a suspected virus is received.

Staff should not attempt to compromise or gain access to restricted areas of the network or to any password-protected information unless they are specifically authorised to do so.

Misuse of the School's computer systems may result in disciplinary action up to and including summary dismissal. For further guidance on what constitutes misuse please see the section entitled Inappropriate Use of the School's Systems and guidance under "Email etiquette and content" below.

Email etiquette and content

Email is a vital business tool, but often lapses inappropriately into an informal means of communication and should therefore be used with great care and discipline.

The School's email facility is intended to promote effective communication within the business on matters relating to the School's business activities and access to the School's email facility is provided for work purposes only.

Staff are permitted to make reasonable personal use of the School's email facility and School systems provided such use is in strict accordance with this policy (see Personal Use below) and the policies referred to in it.

The inappropriate personal use of the School's email facility will be treated as a disciplinary offence resulting in disciplinary action up to and including summary dismissal depending on the seriousness of the offence.

Staff should further be aware that any personal use will be treated as use by a member of Staff in their capacity as an employee of the School. The contents of the School's IT resources and communication systems are the School's property. Therefore Staff should have no expectation of privacy in any message, files, data, document, facsimile, post or message or any other kind of information or communications transmitted to, received or printed from or stored and recorded on our electronic information and communications systems.

The School reserves the right to monitor, intercept and review, without further notice Staff activities using the IT resources and communications systems, including but not limited to use of the School's email system, to ensure that our rules are being complied with and for legitimate purposes and that you consent to such monitoring by your acknowledgment of this policy and your use of such resources and systems. This may include without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of transactions, messages, communications, postings, log-ins, recordings and other uses of the systems as well as keystroke capturing and other network monitoring technologies.

The School may store copies of such data or communications for a period of time after they are created and may delete such copies from time to time without notice.

All Staff are advised not to use our IT resources and communications systems for any matter which he or she wishes to be kept private or confidential from the School.

Staff should always consider if email is the appropriate medium for a particular communication. The School encourages all members of Staff to make direct contact with individuals rather than communicate by email wherever possible to maintain and enhance good working relationships.

Messages sent on the email system should be concise and directed only to relevant individuals on a need to know basis. The content and language used in the message must be consistent with the School's best practice.

Emails should never be sent in the heat of the moment or without first checking the content and language and considering how the message is likely to be received.

All members of Staff should remember that emails can be the subject of legal action for example in claims for breach of contract, confidentiality, defamation, discrimination, harassment etc against both the member of Staff who sent them and the School. Staff should take care with the content of email messages, as incorrect or improper statements can give rise to personal liability of Staff and to liability of the School in the same way as the contents of letters or faxes.

Email messages may of course be disclosed in legal proceedings in the same way as paper documents. Deletion from a user's inbox or archives does not mean that an email is obliterated and all email messages should be treated as potentially retrievable, either from the main server or using specialist software. This should be borne in mind when considering whether email is an appropriate forum of communication in the circumstances of the case and if so the content and language used.

Staff should assume that email messages may be read by others and not include in them anything which would offend or embarrass any reader, or themselves, if it found its way into the public domain. The School standard disclaimer is automatically included on every email.

Staff should ensure that they access their emails at least once every working day, stay in touch by remote access when travelling or working out of the office and should use an out of office response when away from the office for more than a day.

Members of Staff are strictly forbidden from sending abusive, obscene, discriminatory, racist, harassing, derogatory or defamatory messages. If such messages are received, they should not be forwarded and should be reported to a member of the Senior Leadership Team immediately.

If you feel that you have been harassed or bullied, or are offended by material sent to you by a colleague via email, you should inform your Line manager/Head of Department or the Head Teacher who will usually seek to resolve the matter informally. You should refer to our Equal Opportunities and Diversity Policy and the Anti-Harassment and Bullying Policy for further information and guidance.

If an informal procedure is unsuccessful, you may pursue the matter formally under the School's formal grievance procedure. (Further information is contained in the School's Equal Opportunities and Diversity Policy, Anti-Harassment and Bullying Policy and Grievance Policy and Procedure.)

As general guidance, Staff must not:

- Send any email, including re-sending and forwarding, containing sexually explicit or otherwise offensive material either internally or externally;
- Send or forward private emails at work which they would not want a third party to read;
- Send or forward chain mail, junk mail, either within or outside the School;
- Contribute to system congestion by unnecessarily copying or forwarding emails to those who do not have a real need to receive them;

- Sell or advertise using the systems.
- Agree to terms, enter into contractual commitments or make representations by email unless the appropriate authority has been obtained. A name typed at the end of an email is a signature in the same way as a name written in ink at the end of a letter;
- Download or email text, music and other content on the internet subject to copyright protection, unless it is clear that the owner of such works allows this;
- Send messages containing any reference to other individuals or any other business that may be construed as libellous;
- Send messages from another worker's computer or under an assumed name unless specifically authorised;
- Send confidential messages via email or the internet, or by other means of external communication which are known not to be secure;

The School recognises that it is not always possible to control incoming mail. Any material which would be considered as inappropriate or unprofessional, sexually explicit or offensive should be deleted at once.

Any member of Staff who finds that they are receiving such communications from known sources is responsible for contacting that source in order to request that such communication is not repeated.

Staff who receive an email which has been wrongly delivered should return it to the sender of the message. If the email contains confidential information or inappropriate material (as described above) it should not be disclosed or forwarded to another member of Staff or used in any way. Your Line Manager/CTL or the Head Teacher should be informed as soon as reasonably practicable.

Use of the web and the internet

When a website is visited, devices such as cookies, tags or web beacons may be employed to enable the site owner to identify and monitor visitors. If the website is an inappropriate one such a marker could be a source of embarrassment to the School, especially if a member of Staff has accessed, downloaded, stored or forwarded inappropriate material from the website. Staff may even be committing a criminal offence if, for example, the material is pornographic in nature.

Staff must not therefore access from the School's system any web page or any files (whether documents, images or other) downloaded from the web which, on the widest meaning of those terms, could be regarded as illegal, offensive, in bad taste or immoral. While content may be legal in the UK it may be in sufficient bad taste to fall within this prohibition.

As a general rule, if any person within the School (whether intending to view the page or not) might be offended by the contents of a page, or if the fact that the School's software has accessed the page or file might be a source of embarrassment if made public, then viewing it will be a breach of this policy.

Remember also that text, music and other content on the internet are copyright works. Staff should not download or email such content to others unless certain that the owner of such

works allows this.

The School's website is intended to convey our core values and excellence in the educational sector. All members of Staff are encouraged to give feedback concerning the site and new ideas and inclusions are welcome. All such input should be submitted to the Senior Leadership Team in the first instance.

Personal use of the School's systems

The School permits the reasonable use of its internet, email and telephone systems to send personal email, browse the web and make personal telephone calls subject to the provisions set out in this policy.

In addition to the provisions set out above, the following conditions must also be met for personal usage to continue:

a) use must be minimal and take place substantially out of normal working hours (that is, during the member of Staff's usual break time or shortly, before or after normal working hours);
b) use must not interfere with business or office commitments;
c) use must not commit the School to any marginal costs;
d) use must comply at all times with the rules and guidelines set out in this policy;
e) use must also comply with the School's complement of operational policies and procedures including but not limited to, the Equal Opportunities and Diversity Policy, Anti-Harassment and Bullying Policy, Data Protection Policy and Code of Conduct.

The School reserves the right to restrict or prevent access to certain telephone numbers or internet sites if it considers that personal use is excessive or otherwise in breach of this policy.

Inappropriate use of equipment and systems

Misuse or abuse of our telephone or email system or inappropriate use of the internet in breach of this policy will be dealt with in accordance with the School's Disciplinary Policy and Procedure.

Misuse of the internet may, in certain circumstances, constitute a criminal offence. In particular, misuse of the email system or inappropriate use of the internet by viewing, accessing, transmitting or downloading any of the following material, or using any of the following facilities, will amount to gross misconduct (this list is not exhaustive):

a) Accessing pornographic material (that is writings, pictures, films, video clips of a sexually explicit or arousing nature), racist or other inappropriate or unlawful materials;
b) transmitting a false and/or defamatory statement about any person or organisation;
c) sending, receiving, downloading displaying or disseminating material which is discriminatory, offensive, derogatory or may cause offence and embarrassment or harass others;
d) transmitting confidential information about the School and any of its Staff, students or associated third parties;
e) transmitting any other statement which is likely to create any liability (whether criminal or

civil, and whether for the employee or for the School);

f) downloading or disseminating material in breach of copyright;
g) copying, downloading, storing or running any software without the express prior authorisation of a member of the Senior Leadership Team;
h) engaging in online gambling;
i) forwarding electronic chain letters and other materials;
j) accessing, downloading, storing, transmitting or running any material that presents or could present a risk of harm to a child.

Any such action will be treated very seriously and may result in disciplinary action up to and including summary dismissal.

Where evidence of misuse is found the School may undertake a more detailed investigation in accordance with our Disciplinary Policy and Procedure, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or members of management involved in the disciplinary procedure.

If necessary such information may be handed to the police in connection with a criminal investigation.

11. Staff Social Media Protocol

The internet provides a range of social media tools that allow users to interact with one another, for example from rediscovering friends on social networking sites such as Facebook to keeping up with other people's lives on Twitter and maintaining pages on internet encyclopaedias such as Wikipedia.

While recognising the benefits of these media for new opportunities for communication, this policy sets out the principles that Cotham School and contractors are expected to follow when using social media.

It is crucial that children, students, parents and the public at large have confidence in the school's decisions and services. The principles set out in this policy are designed to ensure that staff members use social media responsibly so that confidentiality of children, students and other staff and the reputation of the school are safeguarded.

Cotham School's official means of communication via social media are our whole school Twitter, Faculty accounts and our Facebook account. These are:

Whole School Social Media Pages:

School Facebook - https://www.facebook.com/CothamS
School Twitter - https://www.twitter.com/CothamSchool

Stoke Lodge Playing Fields Facebook - https://www.facebook.com/StokeLodgePlayingField
Stoke Lodge Playing Fields Twitter - https://www.twitter.com/StokeLodgePF

Faculty Social Media Pages:

Design Technology - https://twitter.com/CothamDT
Food Science and Nutrition - https://www.twitter.com/cothamfood
Geography - https://www.twitter.com/CothamGeography
History - https://www.twitter.com/Cotham_History
KS5 English - https://www.twitter.com/EFMCotham
Library - https://www.twitter.com/Cotham_Library
PE - https://www.twitter.com/CothamPE
Performing Arts - https://www.twitter.com/ArtsCotham
Visual Arts - https://www.instagram.com/Cotham_Visual_Arts
Year 8 - https://www.twitter.com/8Cotham

Staff members must be conscious at all times of the need to keep their personal and professional lives separate.

Scope

This policy applies to Cotham School governing body, all teaching and other staff employed directly by the school, external contractors providing services on behalf of the school (for clarification these are companies or individuals where a formal contractual relationship exists), teacher trainees and other trainees, such as apprentices and internships, volunteers (for clarification, volunteers are those that have been designated as such through the

schools formal volunteer procedure) and other individuals who work for or provide services on behalf of the school. These individuals are collectively referred to as ‘staff members’ in this policy.

This policy does not form part of the terms and conditions of employees’ employment with the School and is not intended to have contractual effect. It does however set out the School’s current practices and required standards of conduct and all staff are required to comply with its contents. Breach of the provisions of this policy will be treated as a disciplinary offence which may result in disciplinary action up to and including summary dismissal in accordance with the School’s Disciplinary Policy and Procedure.

This policy covers personal use of social media as well as the use of social media for official school purposes, including but not limited to sites hosted and maintained on behalf of the school. This policy applies to personal webspace such as social networking sites (for example Facebook, MySpace), blogs, microblogs such as Twitter, chatrooms, forums, podcasts, open access online encyclopaedias such as Wikipedia, social bookmarking sites such as del.icio.us and content sharing sites such as Flickr, Instagram, Snapchat and YouTube. The internet is a fast moving technology and it is impossible to cover all circumstances or emerging media - the principles set out in this policy must be followed irrespective of the medium.

Legal Framework

Cotham School is committed to ensuring that all staff members provide confidential services that meet the highest standards.

All individuals working on behalf of the school are bound by a legal duty of confidence and other laws to protect the confidential information they have access to during the course of their work. Disclosure of confidential information on social media is likely to be a breach of a number of laws and professional codes of conduct, including:

- the Human Rights Act 1998
- Common law duty of confidentiality, and
- The Data Protection Act 2018.

Confidential information includes, but is not limited to:

- Person-identifiable information, e.g. pupil and employee records protected by the Data Protection Act 2018
- Information divulged in the expectation of confidentiality
- School business or corporate records containing organisationally or publicly sensitive information
- Any commercially sensitive information such as information relating to commercial proposals or current negotiations, and
- Politically sensitive information.

Staff members should also be aware that other laws relating to libel, defamation, harassment and copyright may apply to information posted on social media, including:

- Libel Act 1843

- Defamation Acts 1952 and 1996
- Protection from Harassment Act 1997
- Criminal Justice and Public Order Act 1994
- Malicious Communications Act 1998
- Communications Act 2003, and
- Copyright, Designs and Patents Act 1988.

Cotham School could be held vicariously responsible for acts of their employees in the course of their employment. For example, staff members who harass co-workers online or who engage in cyberbullying or discrimination on the grounds of race, sex, disability, etc. or who defame a third party while at work may render Cotham School liable to the injured party.

Related Policies

This policy should be read in conjunction with the following school policies:

- Staff Code of Conduct for Employees
- Electronic Information and Communications Systems Policy
- Online Safety policy
- Child Protection and Safeguarding Policies
- Data Protection Policy
- Discrimination and Harassment Policy
- Monitoring Policy

Principles

Social media should never be used in a way that breaches any of our other policies. If an internet post would breach any of our policies in another forum, it will also breach them in an online forum.

The school has its own official school social media sites and only these sites and accounts are authorised to speak on behalf of the school. These sites are:

For example, employees are prohibited from using social media to:

- breach our Electronic Information and Communications Systems policy;
- breach our obligations with respect to the rules of relevant regulatory bodies;
- breach any obligations they may have relating to confidentiality;
- breach our Disciplinary Rules;
- defame or disparage the School, its Staff, its students or parents, its affiliates, partners, suppliers, vendors or other stakeholders;
- harass or bully other staff in any way or breach our Anti-harassment and bullying policy;
- unlawfully discriminate against other staff or third parties or breach our Equal opportunities policy;
- breach our Data protection policy (for example, never disclose personal information about a colleague online);
- breach any other laws or ethical standards (for example, never use social media in a false or misleading way, such as by claiming to be someone other than yourself or by making misleading statements).

Staff should never provide references for other individuals on social or professional networking sites, as such references, positive and negative, can be attributed to the School and create legal liability for both the author of the reference and the organisation.

Staff who breach any of the above policies will be subject to disciplinary action up to and including termination of employment.

Staff must be conscious at all times of the need to keep their personal and professional lives separate. Staff should not put themselves in a position where there is a conflict between their duties to and work for the school and their personal interests.

Staff must not engage in activities involving social media which might bring Cotham School into disrepute.

Staff must not represent their personal views as those of Cotham School on any social medium.

Staff must not discuss personal information about pupils, Cotham School or staff and other professionals they interact with as part of their job on social media.

Staff must not use social media and the internet in any way to attack, insult, abuse or defame pupils, their family members, colleagues, other professionals, other organisations, Cotham School or other organisations connected to Cotham School.

Only staff expressly authorised in advance in writing by the Head Teacher may create or alter any online sources of information on behalf of Cotham School.

Personal use of social media

Personal use of social media outside of work time and/or via other computers, networks. IT resources and communication systems must adhere to the rules and requirements set out in this policy.

Staff members must not have any private personal social contact through any personal social medium with any pupil, whether from Cotham School or any other school, unless the children or students are members of Staff's own family members.

Cotham School does not expect staff members to discontinue contact with their family members via personal social media once the school starts providing services for them. However, any information staff members obtain in the course of their employment must not be used for personal gain nor be passed on to others who may use it in such a way.

Staff members must not have any contact with children's or students' family members through personal social media if that contact is or is likely to constitute or create a conflict of interest, call into question their objectivity or otherwise be in breach of any of the School's rules, policies and procedures.

If Staff members wish to communicate with children or students through social media sites or to enable children or students to keep in touch with one another, they can only do so when the same standards of online safety can be guaranteed and with the advance express

written approval of the Head Teacher.

Staff members must decline ‘friend requests’ from children or students they receive into their personal social media accounts.

On leaving Cotham School’s service, staff members must not contact Cotham School’s children or students by means of personal social media sites. Similarly, staff members must not contact children or students from their former schools by means of personal social media.

Information staff members have access to as part of their employment, including personal information about children or students and their family members, colleagues, staff and other parties and school must not be disclosed or discussed on their or any other personal web space.

Photographs, videos or any other types of image of children or students and their families, or images depicting staff members wearing school uniforms, or clothing with school logos or images identifying sensitive school premises, must not be published on personal web space.

School email addresses and other official contact details must not be used for setting up personal social media accounts or to communicate through such media.

Staff members must not edit open access online encyclopaedias such as Wikipedia in a personal capacity at work. This is because the source of the correction will be recorded as the employer’s IP address and the intervention will, therefore, appear as if it comes from the employer itself.

Cotham School corporate, service or team logos or brands must not be used or published on personal web space.

Caution is advised when inviting work colleagues to be ‘friends’ in personal social networking sites. Social networking sites blur the line between work and personal lives and it may be difficult to maintain professional relationships or it might be just too embarrassing if too much personal information is known in the workplace.

Staff members are strongly advised to ensure that they set the privacy levels of their personal sites as strictly as they can and to opt out of public listings on social networking sites to protect their own privacy. Staff members should keep their passwords confidential, change them often and be careful about what is posted online; it is not safe to reveal home addresses, telephone numbers and other personal information. It is a good idea to use a separate email address just for social networking so that any other contact details are not given away.

Using Social Media on Behalf of Cotham School

Staff members can only use official school sites for communicating with pupils or to enable children and students to communicate with one another. Any such use must be in strict accordance with the rules and provisions of this policy and the related policies referred to in it.

Staff must not create publicly accessible sites that can be associated with the school unless they are expressly authorised to do so by either the Head Teacher. There must be a strong pedagogical or business reason for creating official school sites to communicate with children and students or others and any member of staff wishing to create such a site must set out a proposal to the Head Teacher in accordance with the provisions in this policy.

Staff members who are expressly authorised to create such a site must at all times act in the best interests of children and young people when creating, participating in or contributing content to social media sites.

Monitoring of internet use

The contents of our IT resources and communications systems are the School's property. Therefore staff should have no expectation of privacy in any message, files, data, document, facsimile, telephone conversation, social media, post conversation or message or any other kind of information or communications transmitted to, received or printed from, or stored or recorded on our electronic information and communications systems.

The School reserves the right to monitor, intercept and review, without further notice, staff activities using our IT resources and communication systems, including but not limited to social media posting and activities, to ensure that our rules are being complied with and for legitimate business purposes and you consent to such monitoring by acknowledgment of this policy and your use of such resources and systems.

This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving, and printing transactions, messages, communications, postings, log ins, recordings and other uses of the systems as well as keystroke capturing and other network monitoring technologies.

The School may store copies of such data or communications for a period of time after they are created and may delete such copies from time to time without notice.

All Staff are advised not to use our IT resources and communication systems for any matter that he or she wishes to be kept private or confidential from the School.

Breaches of the Policy

All members of Staff must inform the Head teacher immediately of any breaches of this policy so that appropriate action can be taken promptly to protect the School, its staff, pupils, family members and affiliated providers.

Any breach of this policy may lead to disciplinary action being taken against the staff member/s involved in line with Cotham School up to and including summary dismissal for gross misconduct depending on the seriousness of the breach.

Creation of Publically Accessible Sites

Staff members participating in social media for work purposes are expected to demonstrate the same high standards of behaviour as when using other media or giving public presentations on behalf of Cotham School.

No member of staff may create or administer a publicly accessible site without the express advance written permission of either the Head Teacher.

Prior to creating a site, careful consideration must be given to the following factors:

1. The purposes for using social media and whether the overall investment is likely to be worthwhile for achieving the proposed pedagogical outcome.
2. The proposed audience and level of interactive engagement with the site, for example whether children, students, school staff or members of the public will be able to contribute content to the site,
3. How much time and effort they are willing to commit to the proposed site. They should be aware that maintaining a site is not a one-off task, but involves a considerable time commitment.
4. The potential risks to the School and to any users of the proposed site
5. The methods by which compliance with this policy and the policies referenced within it can be secured and maintained.
6. The time frame during which the site will run
7. The proposed method to ensure that the site is adequately maintained.
8. The proposed exit strategy
9. The proposed method of evaluating the site's success in achieving its proposed objectives.

The Head Teacher and Business Manager will consider your representations on this point whilst also assessing the likely benefit to risk ratio to your proposal before making a decision.

12. Personal Data Handling Protocol

Introduction

Schools should do everything within their power to ensure the safety and security of any material of a personal or sensitive nature (– Good Practice in information handling in schools – keeping data secure, safe and legal – Sept 2008).

It is the responsibility of all members of Cotham School to take care when handling, using or transferring personal data that it cannot be accessed by anyone who does not have permission to have access to that data.

Any loss of personal data can have serious effects for individuals and / or institutions concerned, can bring the school into disrepute and may well result in disciplinary action and / or criminal prosecution. 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 legislation.

The Data Protection Act (2018) lays down a set of rules for processing of personal data (both structured manual records and digital records). It provides individuals (data subjects) with rights of access and security and requires users of data (data processors) to be open about how it is used and to follow “good information handling principles”.

Information Risk Management is a very new issue for schools to tackle and many of the systems required to support it are under development and not yet available. This policy reflects the aims of managing Information Risk whilst the practicalities of how we do it need to be tackled as this work develops.

Cotham School will hold the minimum personal information necessary to enable it to perform its function and information will be erased once the need to hold it has passed.

Every effort will be made to ensure that information is accurate, up to date and that inaccuracies are corrected without unnecessary delay.

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 and carers eg names, addresses, contact details, legal guardianship / contact details, health records, disciplinary records
- Curricular / academic data eg class lists, pupil / student progress records, reports, references
- Professional records eg 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

Cotham School needs to identify a Data Protection Officer whose role will include Information Risk Management. They 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
- identify the Information Asset Owners (IAOs)

Cotham 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 and for what purpose
- how information has been amended or added to over time
- who has access to protected data and why

Everyone in Cotham 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

Cotham School is registered as Data Controllers on the Data Protection Register held by the Information Commissioner.

Information to Parent/Carers – the "Fair Processing Notice"

Under the "Fair Processing" requirements in the Data Protection Act, Cotham School will inform parents/carers of all students of the data they hold on the students, the purposes for which the data is held and the third parties (eg, examination boards, etc) to whom it may be passed. This fair processing notice will be passed to parents/carers by student post. Parents/carers of young people who are new to the school will be provided with the fair processing notice in the induction pack.

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
- Online Safety policy in the staff handbook.
- Staff meetings / briefings / Inset as required
- Day to day support and guidance from Information Asset Owners

Appendix 1 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 and adults Allowed	Staff and adults allowed at certain times	Staff and adults allowed for selected staff	Staff and adults not allowed	Students Allowed	Students allowed at certain times	Students allowed with staff permission	Students not allowed
Mobile phones may be brought to school	✓						✓	
Use of mobile phones in lessons for school use.	✓						✓	
Use of mobile phones in lessons for social use.				✓			✓	
Use of mobile phones in social time	✓							✓
Taking photos on mobile phones or other camera devices		✓					✓	
Use of hand held devices eg PDAs, PSPs	✓							✓
Use of personal email addresses in school, or on school network	✓					✓		
Use of school email for personal emails		✓				✓		
Use of chat rooms / facilities		✓					✓	
Use of instant messaging	✓						✓	
Use of social networking sites		✓						✓
Use of blogs	✓						✓	

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

- The school's gmail system has a complete set of spam and anti-virus warnings. All communications are achieved.
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the Designated Safeguarding Lead, the receipt of any

email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.

- Any digital communication between staff and students or parents / carers (email, chat, etc) must be professional in tone and content. These communications may only take place on official (monitored) Cotham School systems.
- Students should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the Cotham School website and only official email addresses should be used to identify members of staff.

Appendix 2 Unsuitable / inappropriate activities

This table is designed to help illustrate what activities are unacceptable, or in which situations they might be acceptable for certain users. This listing is not exhaustive.

	Acceptable	Acceptable at certain times with approval	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					✓
Adult material that potentially breaches the Obscene Publications Act in the UK					✓
Criminally racist material in the UK					✓
Pornography				✓	✓
Promotion of any kind of discrimination					✓
Promotion of racial or religious hatred					✓
Threatening behaviour, including promotion of physical violence or mental harm					✓
Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrupt				✓	
Using school systems to run a private business		✓			
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the ISP and/or the school				✓	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					✓

Revealing or publicising confidential or proprietary information (eg. financial/personal information, databases, computer/network access codes and passwords				✓	
Creating or propagating computer viruses or other harmful files					✓
Carrying out sustained or instantaneous high volume network traffic (downloading/uploading files) that causes network congestion and hinders others in their use of the internet				✓	
On-line gaming (educational)		✓			
Online gaming (non educational)		✓			
Online gambling				✓	
Online shopping/commerce			✓		
File sharing	✓				
Use of social networking sites		✓			
Use of video broadcasting eg.Youtube	✓				

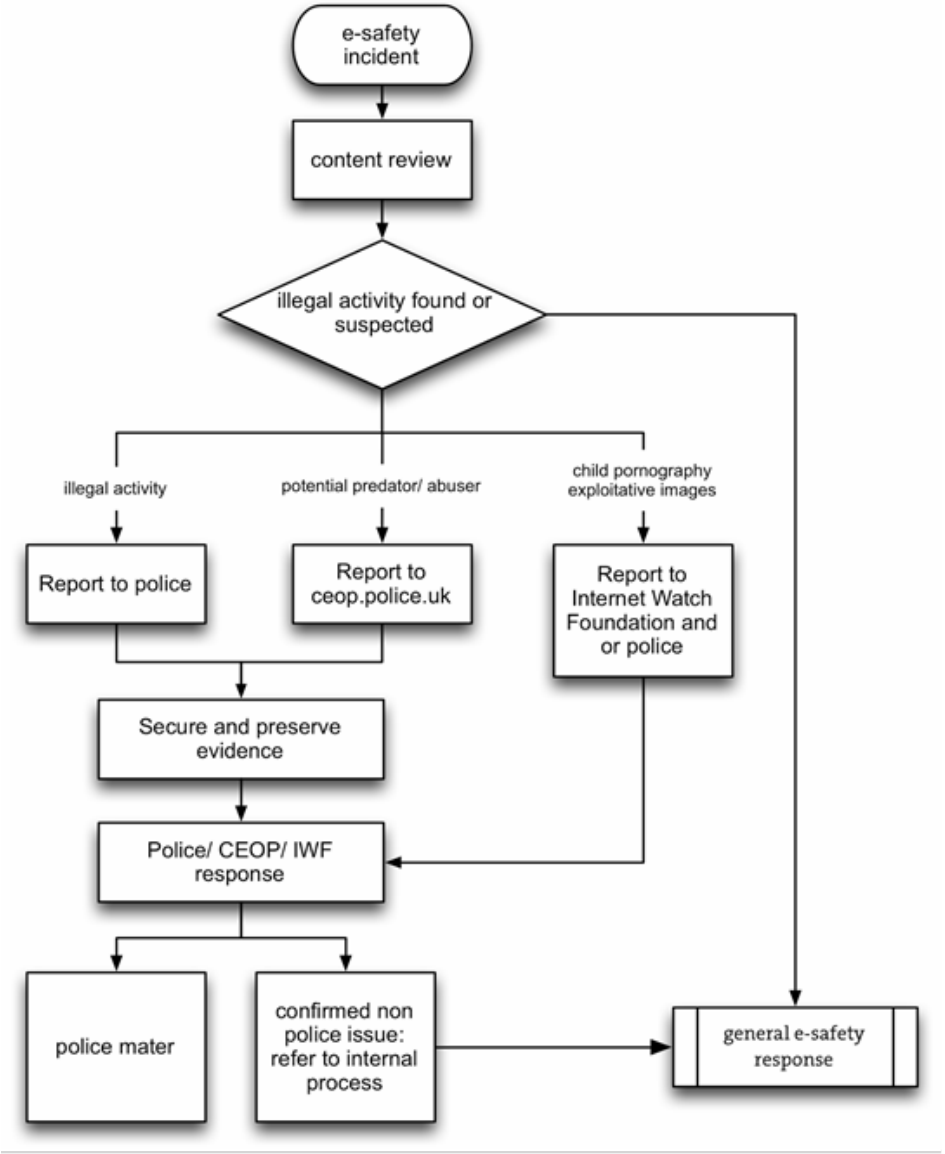
Appendix 3 Responding to incidents of illegal misuse

Flowchart

It is hoped that all members of Cotham School will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity ie.

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials



Appendix 4 Responding to incidents of misuse – students

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

Students

Incidents	Refer to class teacher / tutor	Refer to Head of Department / DSD	Refer to SLT	Refer to e- safety officer	Refer to DSL/ police	Inform parent/ carer	Monitoring and possible restriction	Issue e-safety warning and sanction
Deliberate access to pornographic material		✓		✓	✓	✓	✓	✓
Deliberate access to images involving the sexual abuse of children		✓		✓	✓	✓	✓	✓
Unauthorised use of non- educational sites during lessons	✓							
Unauthorised use of mobile phone / digital camera / other handheld device		✓						✓
Unauthorised use of social networking / instant messaging / personal email								✓
Unauthorised downloading or uploading of files						✓	✓	✓
Allowing others to access school network by sharing username and passwords						✓		✓

Attempting to access or accessing the school network, using another student's account						✓		✓
Attempting to access or accessing the school network, using the account of a member of staff		✓					✓	✓
Corrupting or destroying the data of other users	✓	✓				✓	✓	✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✓	✓		✓		✓	✓	✓
Continued infringements of the above, following previous warnings or sanctions			✓	✓		✓		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		✓		✓			✓	✓
Using proxy sites or other means to subvert the school's filtering system							✓	✓
Accidentally accessing offensive or pornographic material and failing to report the incident						✓		

Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act						✓	✓	✓

Appendix 5 Responding to incidents of misuse – Staff

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

Staff

Incidents:	Refer to line manager	Refer to SLT	Refer to DSL r/ police	Refer to e- safety officer	warning	suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	✓			✓	✓	potentially	potentially
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	✓			✓	✓	potentially	potentially
Unauthorised downloading or uploading of files	✓			✓	✓	potentially	potentially
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	✓			✓	✓	potentially	potentially
Careless use of personal data eg holding or transferring data in an insecure manner	✓			✓			
Deliberate actions to breach data protection or network security rules	✓	✓		✓	potentially	potentially	potentially
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	✓	✓		✓	✓	potentially	potentially

Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✓	✓		✓	✓	potentially	potentially
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students	✓	✓	✓	✓	✓	potentially	potentially
Actions which could compromise the staff member's professional standing	✓	✓				potentially	potentially
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✓	✓				potentially	potentially
Using proxy sites or other means to subvert the school's filtering system	✓	✓		✓		potentially	potentially
Accidentally accessing offensive or pornographic material and failing to report the incident	✓		✓	✓		potentially	potentially
Deliberately accessing or trying to access offensive or pornographic material		✓	✓	✓		potentially	potentially
Breaching copyright or licensing regulations	✓	✓		✓		potentially	potentially
Continued infringements of the above, following previous warnings or sanctions		✓	✓			✓	✓

Appendix 6 Student Acceptable Use Policy Agreement

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools 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. 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 school ICT 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 will have good access to ICT to enhance their learning and will, in return, expect the students to agree to be responsible users.

Acceptable Use Agreement

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

For my own personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I will treat my username and password with care – I will not share it, nor will I try to use any other person's username and password.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line.
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

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

I understand that the school ICT systems are primarily intended for educational use and that:

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

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

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

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

- I will only use my personal electronic devices in school if I have permission. I understand that,if I do use my own devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any attachments to emails, unless I know and trust the person / organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programmes.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings (with the exception of computer workshops) .
- I will only use chat and social networking sites with permission and at the times that are allowed and always in the context of learning.

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

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

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

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be

subject to disciplinary action. This may include loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involving the police.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement.

Upper School Student Acceptable Use Agreement Form

This form relates to the Student Acceptable Use Agreement, to which it is attached.

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

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

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

Name of Student

Group / Class

Signed

Date

Appendix 7

Staff (and Volunteer –for clarification, the term volunteer refers to those that have been designated as such through the schools formal volunteer procedure) Acceptable Use Policy Agreement

New technologies have become integral to the lives of children and young people in today's society, both within schools 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 Cotham School 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.

Cotham 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 learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

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

For my professional and personal safety:

- I understand that Cotham School will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules summarised in this agreement and detailed in the online safety policy also apply to use of Cotham School ICT systems (e.g. laptops, email, etc) out of school.
- I understand that Cotham School ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will be professional in my communications and actions when using school ICT systems:

    - I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
    - I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
    - I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on Cotham School website) it will not be possible to identify by name, or other personal information, those who are featured.
    - I will only use chat and social networking sites in school in accordance with this policy.
    - I will only communicate with students and parents / carers using official Cotham School systems. Any such communication will be professional in tone and manner.
    - I will not engage in any on-line activity that may compromise my professional responsibilities.

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

- When I use my personal handheld / mobile devices (tablets / laptops / mobile phones / USB devices etc, but not limited to) in school, I will follow the rules set out in this

agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by Cotham School about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.

- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up, in accordance with relevant Cotham School policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act, etc. not limited to) or inappropriate or may cause harm or distress to others.
- I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to Cotham School equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Personal Data Policy.
- I understand that data protection policy requires that any staff or student data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by Cotham School policy to disclose such information to an appropriate authority.
- I will immediately report to the IT Services Team any damage or faults involving equipment or software, however this may have happened.
- When using the internet in my professional capacity or for Cotham School sanctioned personal use: I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that I am responsible for my actions in and out of school:
- I understand that this Acceptable Use Policy applies not only to my work and use of Cotham School ICT equipment in school, but also applies to my use of Cotham School ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment with the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

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

Staff / Volunteer Name

Signed

Date

Appendix 8 Parent/Carer Acceptable Use Guidance

New technologies have become integral to the lives of children and young people in today's society, both within schools 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. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Guidance 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 school ICT 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 ICT to enhance their learning and will, in return, expect the students to agree to be responsible users. A copy of the Student / Pupil Acceptable Use Policy is attached to this guidance, so that parents / carers will be aware of the school expectations of the young people in their care.

Please ensure that your child has signed an Acceptable Use Agreement.

Throughout their schooling at Cotham School they will receive online safety education to help them understand the importance of safe use of ICT – both in and out of school.

The school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. The school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

Your Child's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

Please encourage your child to adopt safe use of the internet and digital technologies at home and feel free to contact the school if you have concerns over your child's online safety.

Appendix 9 Permission Form for use of digital/video images

The use of digital / video images plays an important part in learning activities. Students and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media.

The school will comply with the Data Protection Act 2018 and request parent/carers permission before taking images of their children.

We will also ensure that when images are published that the young people cannot be identified by the use of their names.

Parent/Carers are requested to sign the permission form below to allow the school to take and use images of their children:

Dear Parent/Carer, June 2020

Student's name: _____ Reg Group: _____

Photograph / Video Consent Form

At Cotham School we take safeguarding very seriously, and to help keep children safe we store a photograph(s) of your child on the school's management information system and take security videos around the school using CCTV. We process these pupil images for identification purposes and this is necessary for the safe running of the school.

At Cotham School we sometimes take photographs and videos of students and use these photos and videos on the school's website and on social media, in the school's prospectus and newsletters, and on display boards around school, as well as for wider marketing materials used by the school.

We would like your consent to take photos/videos of your child and use them in the ways described above. If you're not happy for us to do this, that's no problem – we will accommodate your preferences.

Please complete the relevant boxes below, sign and return this form to school.

Please write below:	Yes / No
I am happy for photos/videos of my child to be used on the school website and in social media.	
I am happy for photos/videos of my child to be used in school marketing materials.	
I am happy for photos/videos of my child to be used in the school newsletter	
I am happy for photos/videos of my child to be used in the school prospectus.	
I am happy for photos/videos of my child to be used in internal displays.	
OR	
I am **NOT** happy for the school to use photos/videos of my child.	

(Please note that a safeguarding photo and CCTV will still be processed by the school as this is essential to the safe running of the school, even if permission for photos/videos is not given for other purposes)	

If you change your mind at any time, you can let us know by emailing info@cotham.bristol.sch.uk, or by completing a new Photograph/Video Consent Form (available from school office, or on our website).

If you have any other questions, please get in touch.

Why are we asking for your consent?

You may be aware that there are new data protection rules from May 2018 (GDPR). To ensure we are meeting the new requirements, we need to seek your consent to take and use photos/videos of your child. We really value using photos and videos of students, to be able to showcase what students do in school and show what life at our school is like to others, so we would appreciate you taking the time to give your consent.

Parent or carer's signature: _____

Date: _____