ICT AND E-SAFETY POLICY

POLICY NUMBER & CATEGORY	**QSC/23**	**Quality & Standards**
VERSION NO & DATE	**3**	**November 2017**
RATIFYING COMMITTEE	**Trustee Board Meeting**	
DATE RATIFIED		
ANTICIPATED REVIEW DATE:	**November 2019**	
POLICY LEAD	**Matt Phillips**	
POLICY AUTHOR (if different from above)		

POLICY CONTEXT

- Focus School Cambridge Campus recognises that ICT and the Internet are fantastic tools for learning and communication that can be used in school to enhance the curriculum, challenge students, and support creativity and independence. Using ICT to interact, collaborate and share ideas can benefit everyone in the school community, but it is important that the use of the Internet and ICT is seen as a responsibility and that students, staff and parents use it appropriately and practice outstanding e-safety. It is important that all members of the school community are aware of the dangers of using the Internet and how they should conduct themselves online.

POLICY REQUIREMENT (see Section 2)

- ICT plays a key role in teaching and learning and administrative duties in school. It includes computer technologies, electronic data storage and the fast-growing range of digital communication and information-sharing technologies.
- Use of school ICT by employees, students and other approved users is to be limited to educational, professional development and personal usage appropriate in the School environment. The school reserves the right to monitor access and review all use and to audit at any time any material on the School ICT systems and equipment.
- This policy is available from the school office for parents, staff, and pupils to access as and when they wish. Rules relating to the school code of conduct when online, and e-safety guidelines, are displayed around the school. Online safety is integrated into the curriculum in any circumstance where the Internet or technology are being used, and during PSHE lessons where personal safety, responsibility, and/or development are being discussed.

CONTENTS

1 INTRODUCTION

1.1 Rationale

1.1.1 Online safety covers the Internet but it also covers mobile phones and other electronic communications technologies. We know that some adults and young people will use these technologies to harm children. The harm might range from sending hurtful or abusive texts and emails, to enticing children to engage in sexually harmful conversations or actions online, webcam filming, photography or face-to-face meetings. There is a 'duty of care' for any persons working with children. Educating all members of the school community on the risks and responsibilities of online safety falls under this duty. It is important that there is a balance between controlling access to the internet and technology and allowing freedom to explore and use these tools to their full potential. This policy aims to be an aid in regulating ICT activity in school, and provide a good understanding of appropriate ICT use that members of the school community can use as a reference for their conduct online outside of school hours. Online safety is a whole-school issue and responsibility.

1.1.2 Cyber-bullying by pupils will be treated as seriously as any other type of bullying and will be managed through our anti-bullying procedures, which are outlined in our Anti-Bullying Policy.

1.2 Scope

1.2.1 This Policy and Procedures applies to all staff, including teachers, support staff, trainees, external tutors and providers, trustees, administrative personnel, contractors, visitors, volunteers, all students (including adult and community), and any other individual authorised to make use of the school ICT facilities and equipment.

1.2.2 Students and users not employed by the school may not use the school network facilities and ICT equipment in any circumstances unless in exceptional circumstances and the appropriate Acceptable Use Agreement has been signed and approved by the Lead CA or Head Teacher. This includes the 'Associate WiFi network' for visitors. Acceptable Use Agreements also apply to the use of private ICT equipment on the school site, or at any school-related activity, regardless of its location. This includes off-site access to the school network from school or private equipment.

1.2.3 This Policy has been ratified by the Trustees of Focus Learning Trust.

1.2.4 This Policy does not form part of any member of staff's contract of employment and it may be amended at any time.

1.2.5 This Policy will be reviewed at least every two years or when significant changes to the school's technology use occur.

1.3 Principles

1.3.1 The Internet is used in school to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions. Technology is advancing rapidly and is now a huge part of everyday life, education and business. We want to equip our students with all the necessary ICT skills that they will need in order to enable them to progress confidently into a professional working environment when they leave school.

1.3.2 Focus Learning Trust will share the commitment in assisting campuses to establish a safe, secure platform with approved broadband internet connection, teaching and learning resources and services via Focus IT Support.

1.3.3 Focus School Cambridge Campus maintains an ethos of self-directed and self-organised learning, allowing students to pursue and extend their learning more deeply, widely and to

a higher level. Central to this is highly effective use of technology for students to research, collaborate, communicate and assess their learning.

1.3.4 Our duty is to ensure our students learn to critically evaluate internet content, to adopt responsible behaviour online and to manage concerns effectively and immediately. We will ensure system-wide, consistent, working practices that embrace emerging technologies whilst protecting our staff, students, data and wider community from cyber-crime, unsafe, inappropriate or illegal activity.

2 POLICY

Making use of ICT and the internet in school

2.1 Some of the benefits of using ICT and the Internet in schools are:

For pupils:

2.1.1 Access to worldwide educational resources and institutions such as museums and libraries.

2.1.2 Access to subject experts, inspirational people and organisations. The internet can provide a great opportunity for pupils to learn from people that they otherwise would never be able to access.

2.1.3 An enhanced curriculum; interactive learning tools; collaboration, locally, nationally, and globally; self-evaluation; feedback and assessment; updates on current affairs as they happen.

2.1.4 Access to learning whenever and wherever convenient. Including by video conference platforms.

2.1.5 Freedom to be creative.

2.1.6 Freedom to explore the world and its cultures from within a classroom.

2.1.7 Social inclusion, in class and online.

2.1.8 Access to case studies, videos and interactive media to enhance understanding.

2.1.9 Individualised access to learning.

For staff:

2.1.10 Professional development through access to national developments, educational materials and examples of effective curriculum practice and classroom strategies.

2.1.11 Immediate professional and personal support through networks and associations.

2.1.12 Improved access to technical support.

2.1.13 Ability to provide immediate feedback to students and parents.

2.1.14 Class management, attendance records, schedule, and assignment tracking.

2.2 Learning to Evaluate Internet Content

2.2.1 With so much information available online it is important that pupils learn how to evaluate Internet content for accuracy and intent. This is approached by the school as part of digital literacy across all subjects in the curriculum. Students will be taught to:

- Be critically aware of materials they read, and shown how to validate information before accepting it as accurate
- Use age-appropriate tools to search for information online

- Acknowledge the source of information used and to respect copyright. Plagiarism is against the law and the school will take any intentional acts of plagiary very seriously. Students who are found to have plagiarised will be disciplined. If they have plagiarised in an exam or a piece of coursework, they may be prohibited from completing that exam.

2.3 Monitoring and filtering

2.3.1 ICT authorised staff , (Authorised staff are the ICT Manager, Lead CA, Headteacher and Focus ICT Support) may inspect any school ICT equipment including monitoring, intercepting, accessing records and telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice, video or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain school business related information; to confirm or investigate compliance with school policies, standards and procedures; to ensure the effective operation of school ICT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime.

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

2.3.3 All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act 1998

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

2.3.5 All e-mails are logged and filtered by the National Support Office and any infringements notified to the Lead CA.

2.3.6 The IT Manager, Lead CA or Headteacher may request (via Focus IT helpdesk) additional support to monitor students as required.

2.3.7 Staff should have no expectation of privacy in any information or communications transmitted to, received or printed from, or stored or recorded on the school's electronic and information and communication systems.

Focus IT Support ensures that:

2.3.8 We use specialist software to constantly monitor all e-mail and internet activity in school. E-mail text is monitored using a ‘Secure E-mail Gateway’ with profanity filter.

2.3.9 All Focus Campus computers are pre-loaded with web filtering and monitoring software provided by Streamline 3.

2.3.10 Website URLs are managed using a Dynamic Whitelisting approach.

2.3.11 This limits use with a 'deny by default' approach so that only Focus Learning Trust approved files or applications can be installed and only approved websites may be accessed by staff and students. Dynamic application whitelisting prevents unsafe or inappropriate browsing.

2.3.12 The whitelisting software is preconfigured with trusted, appropriate domains. Staff can request more required domains as needed. The Focus Schools’ National Support Office whitelisting team act as the gatekeepers for safe searching, by checking and approving each request.

2.3.13 All content, including that approved by staff, is checked against a unique database in which almost every known URL is categorised according to its subject matter and age-appropriateness. Harmful web-content and processes – such as violence, pornography, gambling, social media, apps, chat rooms, games, non-Focus e-mail and search engines are restricted or obstructed.

2.3.14 A fire-wall prevents malicious software and other unapproved programs from running.

2.3.15 Filtering is not limited to filtering web traffic and also includes the blocking of inappropriate content via mobile and app technologies.

2.3.16 There are automated and manual reporting and alert systems to identify breaches or attempted breaches of network security, data security, downloads, software use and online activity.

2.3.17 Parents and the school receive a weekly report to summarise students' browsing. This will alert our Focus ICT Team to incidents involving:

- Peer on peer including cyberbullying
- Grooming, radicalisation and sexual threats
- Inappropriate behaviour on social media
- Racist, homophobic or extreme language
- Inadvertent or deliberate access to inappropriate web contents, such as sites dealing with sex or violence
- Access to online gambling or shopping sites

2.3.18 Year 12 and 13 students have a school e-mail address, with other year groups to follow. The acceptable use agreement requires parents and carers to have their children's school e-mail set up on their own account, so all e-mails may be monitored. Non-Focus e-mail is obstructed on Focus devices and should not be accessed.

2.3.19 Upon a software alert to any harmful content or behaviour, the student concerned will be identified and a screenshot of the activity created. This will allow senior leaders to assess the content and level of severity and to take appropriate action.

2.3.20 The Focus ICT Team will follow the Flowchart of Managing E-Safety Incidents in section 3.0

2.4 E-Safety Reporting Button

2.4.1 To ensure students and all other stakeholders have access to a confidential and direct reporting system, we have an e-safety reporting button on the main homepage of our Student Intranet. The button is for reporting concerns about e-safety, bullying, inappropriate use of computers or the internet. It is labelled as such.

2.4.2 Our Reporting Button links to a secure reporting form that automatically alerts the designated safeguarding leads at the Focus School National Support Office. The safeguarding leads at the National Support Office include the Brethren Community safeguarding lead and a non-community safeguarding lead. All incidents will be managed in line with the Focus School Safeguarding Policy.

2.5 ClickView Video Software

2.5.1 Students do not have access to YouTube or other similar video-sharing platforms. Focus Learning Trust uses the ClickView platform to share curriculum-appropriate videos with students.

2.5.2 The ClickView video software categories all content by age-appropriateness, to prevent inappropriate material being watched.

2.5.3 A log-in is required, linked to student's age and year group in school. This restricts viewing to only content which is age-appropriate.

2.5.4 School staff are only permitted to show or share videos to students from the Focus School 'library'. Content in the library has been moderated by the ClickView Librarian and checked for age-appropriateness as well as being appropriate for the National Curriculum

specification for that subject. There must be no video used by any party that undermines the School Ethos, the Values Statement and the Guiding Principles of the School

2.5.5 Staff are not permitted to show or share video material with students that is directly from public sources on ClickView, under any circumstances. The same applies to showing video material directly from any other online video repository such as YouTube, unless a staff member has the express permission of the Lead CA.

2.5.6 The IT Manager will download a weekly ClickView activity report to monitor usage. Breach of the 'library-only' rule will be treated as a disciplinary matter, in contravention of e-safety principles and of the Ethos, the Values Statement and the Guiding Principles of the school.

2.6 Learning Management System

2.6.1 Focus Learning Trust uses a Learning Management System (LMS) to share learning materials between staff and students on all campuses. Access to the LMS is by authenticated log-in for staff and students. Students are enrolled onto a virtual 'course' with other students in their class. This may be within a campus or between campuses if lessons are taught by Video Conferencing. This allows learning to be self-directed and for frequent collaboration between students. The following controls apply to use of the LMS:

- The LMS has a discussion forum that can be switched on by a class teacher, for students specifically in their class. The forum should be moderated by the teacher daily and inappropriate posts managed using the Behaviour Management Policy and Anti-Bullying Policy
- Discussion forums are only switched on when needed, then are blocked for further messages
- Communication between students and staff in discussion forums is covered by the Acceptable Use Agreements for staff and students. Inappropriate use will result in an investigation and appropriate sanctions - as outlined in the Breaches and Incident Reporting section of this policy
- All documents shared are moderated by the class teacher
- The audio feedback function is moderated by the teacher, when used. When not part of directed learning, this function is switched off
- Shared documents, for example via Microsoft OneNote, can be monitored by the IT team at Focus Learning Trust

2.7 Virtual Classroom (VC)

2.7.1 Video Conferencing allows lessons to be conducted via video-link software, to connect a teacher on one campus to students on several other campuses. VC lessons are only permitted with a teacher present to lead the lesson and a staff member to supervise students at the receiving campus. Students are not permitted to conduct a VC lesson or VC link without a staff member to supervise at the delivering and receiving campuses.

2.7.2 The level of supervision should be determined by the Head Teacher as appropriate.

2.8 Managing Information Systems

2.8.1 The school is responsible for reviewing and managing the security of the computers and Internet networks as a whole and takes the protection of school data and personal protection of our school community very seriously. This means protecting the school network, as far as is practicably possible, against viruses, hackers and other external security threats. The IT Technicians/ICT Coordinator/ICT Manager will review the security of the school information systems and users regularly and virus protection software will be updated regularly. Some safeguards that the school takes to secure our computer systems are:

- Ensuring that all personal data sent over the Internet or taken off site is encrypted
- Making sure that unapproved software is not downloaded to any school computers. Alerts will be set up to warn users of this
- Files held on the school network will be regularly checked for viruses
- The use of user logins and passwords to access the school network will be enforced
- Portable media containing school data or programmes will not be taken off-site without specific permission from a member of the senior leadership team.

2.8.2 For more information on data protection in school please refer to our Data Protection Policy. More information on protecting personal data can be found in section 2.13 of this policy.

2.9 Emails

2.9.1 The school uses email internally for staff and pupils, and externally for contacting parents, and is an essential part of school communication.

2.9.2 Staff and pupils should be aware that school email accounts should only be used for school-related matters, ie for staff to contact parents, students, other members of staff and other professionals for work purposes. The school has the right to monitor emails and their contents but will only do so if it feels there is reason to.

2.10 School Email Accounts and Appropriate Use

Staff should be aware of the following when using email in school:

2.10.1 Staff should only use official school-provided email accounts to communicate with pupils, parents, carers or on school business. Personal email accounts should not be used to contact any of these people and should not be accessed during school hours.

2.10.2 Emails sent from school accounts should be professionally and carefully written. Staff are representing the school at all times and should take this into account when entering into any email communications.

2.10.3 Staff must tell their line manager or a member of the senior leadership team if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account. They should not attempt to deal with this themselves.

2.10.4 The forwarding of chain messages is not permitted in school.

Students should be aware of the following when using email in school, and will be taught to follow these guidelines through the ICT curriculum and in any instance where email is being used within the curriculum or in class:

2.10.5 In school, pupils should only use school-approved email accounts

2.10.6 Students will not use personal, non-school, email accounts to communicate with school staff.

2.10.7 Excessive social emailing will be restricted

2.10.8 Pupils should tell a member of staff if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account. They should not attempt to deal with this themselves.

2.10.9 Pupils must be careful not to reveal any personal information over email, or arrange to meet up with anyone who they have met online without specific permission from an adult in charge.

2.10.10 Pupils will be educated through the curriculum to identify spam, phishing and virus emails and attachments that could cause harm to the school network or their personal account or wellbeing.

2.11 Published Content and the School Website

2.11.1 The school website is viewed as a useful tool for communicating our school ethos, policies and practice to the wider community. It is also a valuable resource for parents, students, and staff for keeping up-to-date with school news and events, celebrating whole-school achievements and personal achievements, and promoting school projects.

2.11.2 The website is in the public domain, and can be viewed by anybody online. Any information published on the website will be carefully considered in terms of safety for the school community, copyrights and privacy policies and for safer recruitment. No personal information on staff or pupils will be published, and details for contacting the school will be for the school office only. For information on the school policy on children's photographs on the school website please refer to section 2.12 of this policy.

2.12 Policy and Guidance of Safe Use of Children's Photographs and Work

2.12.1 Colour photographs and pupils work bring our school to life, showcase our student's talents, and add interest to publications both online and in print that represent the school. However, the school acknowledges the importance of having safety precautions in place to prevent the misuse of such material.

2.12.2 Under the Data Protection Act 1998 images of pupils and staff will not be displayed in public, either in print or online, without consent. On admission to the school parents/carers will be asked to sign a photography consent form. The school does this so as to prevent repeatedly asking parents for consent over the school year, which is time-consuming for both parents and the school. The terms of use of photographs never change, and so consenting to the use of photographs of your child over a period of time rather than a one-off incident does not affect what you are consenting to. This consent form will outline the school's policy on the use of photographs of children, including:

- How and when the photographs will be used
- How long parents are consenting the use of the images for
- School policy on the storage and deletion of photographs.

2.12.3 Parents will be contacted annually for consent.

Using photographs of individual children

2.12.4 The vast majority of people who take or view photographs or videos of children do so for entirely innocent, understandable and acceptable reasons. Sadly, some people abuse children through taking or using images, so we must ensure that we have safeguards in place.

2.12.5 It is important that published images do not identify students or put them at risk of being identified. The school is careful to ensure that images published on the school website cannot be reused or manipulated through watermarking and browser restrictions. Only images created by or for the school will be used in public and children may not be approached or photographed while in school or doing school activities without the school's permission. The school follows general rules on the use of photographs of individual children:

2.12.6 Parental consent must be obtained. Consent will cover the use of images in:

- all school publications
- on the school website

- in newspapers as allowed by the school
- in videos made by the school or in class for school projects.
- Electronic and paper images will be stored securely.
- Names of stored photographic files will not identify the child.

2.12.7 Images will be carefully chosen to ensure that they do not pose a risk of misuse. This includes ensuring that pupils are appropriately dressed. Photographs of activities which may pose a greater risk of potential misuse (for example, swimming activities), will focus more on the sport than the pupils (i.e. a student in a swimming pool, rather than standing by the side in a swimsuit).

2.12.8 For public documents, including in newspapers, full names will not be published alongside images of the child. Groups may be referred to collectively by year group or form name.

2.12.9 Events recorded by family members of the students such as school plays or sports days must be used for personal use only.

2.12.10 Pupils are encouraged to tell a member staff if they are concerned or uncomfortable with any photographs that are taken of them or they are being asked to participate in.

2.12.11 Any photographers that are commissioned by the school will be fully briefed on appropriateness in terms of content and behaviour, will wear identification at all times, and will not have unsupervised access to the pupils. For more information on safeguarding in school please refer to our child protection and safeguarding policy.

2.13 Complaints of Misuse of Photographs or Video

2.13.1 Parents should follow standard school complaints procedure if they have a concern or complaint regarding the misuse of school photographs. Please refer to our Complaints Procedure for more information on the steps to take when making a complaint. Any issues or sanctions will be dealt with in line with the school's Child Protection and Safeguarding Policy and Behaviour Management Policy.

2.14 E-Safety

2.14.1 Unfortunately some adults and young people will use technologies to harm children. The harm might range from sending hurtful or abusive texts and emails, to grooming and enticing children to engage in sexually harmful conversations, webcam photography or face-to-face meetings.

2.14.2 Pupils may also be distressed or harmed by accessing inappropriate websites that promote unhealthy lifestyles, extremist behaviour and criminal activity.

2.14.3 Cyberbullying and sexting by pupils will be treated as seriously as any other type of bullying and will be managed through our anti-bullying procedures. Serious incidents may be managed in line with our child protection procedures.

2.14.4 Many pupils own or have access to hand held devices and parents are encouraged to consider measures to keep their children safe when using the internet at home and in the community (See appendices 1, 2 & 3 for acceptable use of ICT in school)

2.14.5 All staff and parents receive online safety training and the school's E-Safety Coordinator is Malcolm Smith

2.15 Social Networking, Social Media and Personal Publishing

2.15.1 Personal publishing tools include blogs, wikis, social networking sites, bulletin boards, chat rooms and instant messaging programmes. These online forums are the more obvious sources of inappropriate and harmful behaviour and where pupils are most vulnerable to being contacted by a dangerous person or subjected to bullying. It is important that we

educate pupils so that they can make their own informed decisions and take responsibility for their conduct online. Pupils are not allowed to access social media sites in school

2.15.2 Social media sites have many benefits for both personal use and professional learning; however, both staff and students should be aware of how they present themselves online. Students are taught through the ICT curriculum and PSHE about the risks and responsibility of uploading personal information and the difficulty of taking it down completely once it is out in such a public place. The school follows general rules on the use of social media and social networking sites in school:

- Pupils are educated on the dangers of social networking sites and how to use them in safe and productive ways. They are all made fully aware of the school's code of conduct regarding the use of ICT and technologies and behaviour online.
- Any sites that are to be used in class will be risk-assessed by the teacher in charge prior to the lesson to ensure that the site is age-appropriate and safe for use.
- Official school blogs created by staff or students/year groups/school clubs as part of the school curriculum will be password-protected and run from the school website with the approval of a member of staff and will be moderated by a member of staff.
- Pupils and staff are encouraged not to publish specific and detailed private thoughts, especially those that might be considered hurtful, harmful or defamatory. The school expects all staff and pupils to remember that they are representing the school at all times and must act appropriately.
- Safe and professional behaviour of staff online will be discussed at staff induction.

2.15.3 Use of social media sites and websites created by students as part of their learning must be in line with the OneSchool Global Online Policy (Appendix 10)

2.16 Mobile Phones and Personal Communication Devices

2.16.1 While mobile phones and personal communication devices are commonplace in today's society, their use and the responsibility for using them should not be taken lightly. Some issues surrounding the possession of these devices are they:

- Can make pupils and staff more vulnerable to cyberbullying, grooming and online abuse
- Can be used to access inappropriate internet material
- Can be a distraction in the classroom
- Are valuable items that could be stolen, damaged, or lost
- Can have integrated cameras, which can lead to child protection, bullying and data protection issues.

2.16.2 The school takes certain measures to ensure that **mobile phones** and **personal communication devices** are used responsibly in school. Some of these are outlined below.

Visitors to Cambridge Campus

- All visitors to the campus will be made aware of the ICT & E-Safety Policy and be asked to turn mobile telephones off during their visit to the campus. A notice to this effect will be on display in the reception area of the school and detailed in the Visitor Policy.
- Should visitors wish to make a telephone call, they will be invited to use the school telephone.

- During the school day Trustees and CAs must only use their phones in areas of the school where students do not have access e.g. school office, staff room etc.

2.16.3 Mobile Phone or Personal Communication Device Misuse

Pupils

- The school will not tolerate cyber bullying against either pupils or staff. Sending inappropriate, suggestive or abusive messages is forbidden and anyone who is found to have sent a message of such content will be subject to disciplinary procedures. For more information on the school's disciplinary sanctions read the school behaviour policy.
- A member of staff can confiscate mobile phones, and a member of the senior leadership team can search the device if there is reason to believe that there may be evidence of harmful or inappropriate use on the device.
- By default, students are not allowed to have mobile telephones or similar devices in school, on school transport or school excursions and parents are required to comply with this policy. Exceptions are below:
- In certain circumstances the school acknowledges that a parent may wish a child to bring a phone to school eg. for security purposes. In such circumstances, a permission slip should be obtained, the phone should be clearly labelled and it should be handed to a teacher on arrival at the school for safety. It will be returned at the end of the school day only.
- Mobile phones will not be allowed on educational visits or short trips away from school. However, students may have their mobile phones when going on longer trips or when required, detailed within a specific risk assessment.
- Urgent communications for members of staff must be directed through the main office during working hours.
- Urgent messages for students must go through the main office and if a student needs to make telephone calls during school hours they must go to the main office for permission.
- Any such items that are brought into school will be confiscated and returned at the end of the school day with a note for the relevant parent to ask that the phone or other device is not brought to school again.
- Pupils who breach school policy relating to the use of personal devices will be disciplined in line with the school's behaviour policy. Their mobile phone may be confiscated.
- Pupils are under no circumstances allowed to bring mobile phones or personal devices into examination rooms with them. If a pupil is found with a mobile phone in their possession it will be confiscated. The breach of rules will be reported to the appropriate examining body and may result in the pupil being prohibited from taking that exam.

Staff

- Staff mobile telephones must be switched off during working hours. Outside of these times, personal phones or communication devices may be used discreetly in the staff room and never in the presence of students. At break time and lunchtime, staff may use personal phones or communication devices discretely in the staffroom.

- The Trustees / Headteacher may agree exceptions to the above, for example when off-site, on training days or taking lessons on the playing field.
- Staff should never contact students or parents from their personal mobile telephone, or give their mobile telephone number to students or parents. If a member of staff needs to make telephone contact with a student or parent, a school telephone should be used. For school visits, this should be a **school-owned** mobile telephone, intended for that purpose.
- Staff should never send to, or accept from, colleagues or students, texts or images that could be viewed as inappropriate.
- Members of staff should never use the camera on their mobile telephone to photograph students or allow themselves to be photographed by a student.
- Any breach of school policy may result in disciplinary action against that member of staff. More information on this can be found in the child protection and safeguarding policy, or in the staff contract of employment.

2.17 Cyberbullying

2.17.1 The school, as with any other form of bullying, takes Cyber bullying very seriously. Information about specific strategies or programmes in place to prevent and tackle bullying is set out in the behaviour policy. The anonymity that can come with using the internet can sometimes make people feel safe to say and do hurtful things that they otherwise would not do in person. It is made very clear to members of the school community what is expected of them in terms of respecting their peers, members of the public and staff, and any intentional breach of this will result in disciplinary action.

2.17.2 In the event of an allegation of cyber-bullying, the school will:

- Take it seriously
- Act as quickly as possible to establish the facts. It may be necessary to examine school systems and logs or contact the service provider in order to identify the bully
- Record and report the incident
- Provide support and reassurance to the victim
- Make it clear to the 'bully' that this behaviour will not be tolerated. If there is a group of people involved, they will be spoken to individually and/or as a whole group. It is important that children who have harmed another, either physically or emotionally, redress their actions and the school will make sure that they understand what they have done and the impact of their actions.

2.17.3 If a sanction is used, it will correlate to the seriousness of the incident and the 'bully' will be told why it is being used. They will be asked to remove any harmful or inappropriate content that has been published, and the service provider may be contacted to do this if they refuse or are unable to remove it. They may have their Internet access suspended in school.

2.17.4 Repeated bullying may result in fixed-term exclusion.

2.18 Managing Emerging Technologies

2.18.1 Technology is progressing rapidly and new technologies are emerging all the time. The school will risk-assess any new technologies before they are allowed in school, and will consider any educational benefits that they might have. The school keeps up-to-date with new technologies and is prepared to quickly develop appropriate strategies for dealing with new technological developments.

2.19 Protecting Personal Data

2.19.1 Focus School Cambridge Campus believes that protecting the privacy of our staff and pupils and regulating their safety through data management, control and evaluation is vital to whole-school and individual progress. The school collects personal data from pupils, parents, and staff and processes it in order to support teaching and learning, monitor and report on pupil and teacher progress, and strengthen our pastoral provision.

2.19.2 We take responsibility for ensuring that any data that we collect and process is used correctly and only as is necessary, and the school will keep parents fully informed of the how data is collected, what is collected, and how it is used. National curriculum results, attendance and registration records, special educational needs data, and any relevant medical information are examples of the type of data that the school needs. Through effective data management we can monitor a range of school provisions and evaluate the wellbeing and academic progression of our school body to ensure that we are doing all we can to support both staff and students.

2.19.3 In line with the Data Protection Act 1998, and following principles of good practice when processing data, the school will:

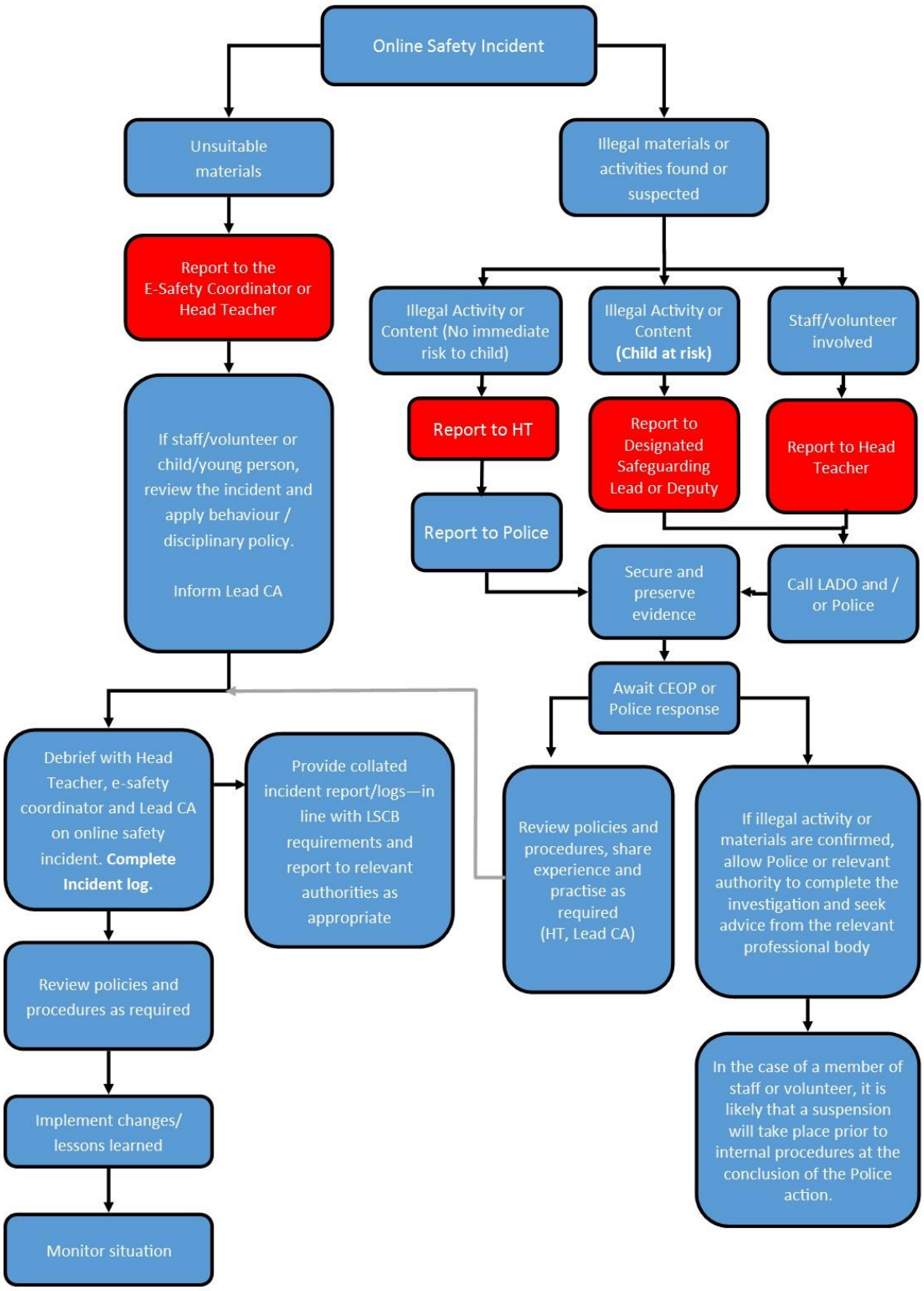
- Ensure that data is fairly and lawfully processed
- Process data only for limited purposes
- Ensure that all data processed is adequate, relevant and not excessive
- Ensure that data processed is accurate
- Not keep data longer than is necessary
- Process the data in accordance with the data subject's rights
- Ensure that data is secure
- Ensure that data is not transferred to other countries without adequate protection.

2.19.4 There may be circumstances where the school is required either by law or in the best interests of our students or staff to pass information onto external authorities; for example, our local authority, Ofsted, or the Department of Health. These authorities are up-to-date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

2.19.5 For more information on the school's safeguards relating to data protection read the school's data protection policy.

3 PROCEDURE

MANAGING E-SAFETY INCIDENTS FLOWCHART



4.0 RESPONSIBILITIES

Post(s)	Responsibilities	Ref
School Trust Board Members	Trustees are responsible for the approval of the ICT & E-Safety Policy and for reviewing the effectiveness of the policy by reviewing e-safety incidents and monitoring reports. Online safety falls within the remit of the trustee responsible for Safeguarding. The role of the online safety trustee will include: • ensure an ICT & E-safety policy is in place, reviewed every 2 years and is available to all stakeholders • ensure that there is an E-Safety Coordinator who has been trained to a higher level of knowledge which is relevant to the school, up to date and progressive • ensure that procedures for the safe use of ICT and the Internet are in place and adhered to • hold the Headteacher and staff accountable for online safety.	
Headteacher and SLT	The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the E-Safety Coordinator. Any complaint about staff misuse must be referred to the E-Safety Coordinator at the school or, in the case of a serious complaint, to the Headteacher. • Ensure access to induction and training in online safety practices for all users. • Ensure appropriate action is taken in all cases of misuse. • Ensure that staff or external providers who operate monitoring procedures be supervised by a named member of SLT. • Ensure that pupil or staff personal data as recorded within school management system sent over the Internet is secured. • The Senior Leadership Team will receive monitoring reports from the E-Safety co-ordinator.	
E-Safety Coordinator	• Leads E-safety meetings. • Work in partnership with the school ICT Manager to ensure systems to protect students are reviewed and improved. • Receives reports of e-safety incidents and creates a log of incidents to inform future online safety developments,	

	• Will be a member of the senior leadership team. All members of the school community, including visitors, will be made aware of who holds this post. • Keep abreast of current issues and guidance and to disseminate this information to the school community. • Liaise with the nominated member of the Trust & Headteacher to provide an annual report on online safety.	
ICT Manager / Technical Staff	The ICT Manager is responsible for ensuring: • That the schools technical infrastructure is secure and is not open to misuse or malicious attack. • That the school meets required online safety technical requirements and any relevant body online safety policy / guidance that may apply. • That users may only access the networks and devices through a properly enforced password protection policy. • The filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person. • That they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant. • That the use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher; E-Safety Coordinator for investigation / action / sanction • That monitoring software / systems are implemented and updated as agreed in school policies.	
Focus ICT Support (based at Focus Learning Trust. Exchange Place, Warwick)	• Ensure that the school's technical infrastructure is secure and is not open to misuse or malicious attack • Ensure that the school meets the required online safety technical requirements in line with the Policy and Handbook • Ensure that users may only access the networks and devices through properly enforced password protection • Ensure that internet filtering methods are appropriate, effective and reasonable and are not the sole responsibility of any single person • Operate monitoring procedures including software systems to ensure systems to protect students are reviewed and improved	

	• Ensure that the use of the network / internet / virtual learning environments / remote access / e-mail is regularly monitored in order that any misuse / attempted misuse can be reported to the Head Teacher ICT Manager / Lead CA for investigation / action • Ensure that any breach is reported to the Headteacher, ICT Manager or if unavailable the Lead CA • Ensure that the ICT Systems are reviewed regularly with regard to security and that virus protection is installed and up-dated regularly • Keep up-to-date with online safety technical information.	

5.0 REFERENCE DOCUMENTS

Anti-Bullying Policy

Behaviour Management Policy

Child Protection & Safeguarding Policy

Data Protection Policy

6.0 GLOSSARY

- **ICT** refers to the term 'Information and Communication Technologies' including all forms of computing, the internet, telecommunications, digital media and mobile telephones.
- **School ICT** refers to the School's computer network, Internet access facilities, computers, and other school ICT, equipment/devices as outlined in the ICT Handbook.
- **Focus IT Support** refers to the Focus Learning Trust National Support Office IT Support for Focus School Cambridge Campus.
- **ICT equipment** used in this document, includes but is not limited to, computers (such as desktops, laptops, PDAs), video conferencing equipment, storage devices (such as USB and flash memory devices, CDs, DVDs, floppy disks, iPods, MP3 players), cameras (such as video, digital, webcams), all types of mobile phones, video and audio players/receivers (such as portable CD and DVD players), and any other, similar, technologies as they come into use.
- **Device:** Digitally capable technology likely capable of wireless or mobile connectivity, including mobile telephones, smart-watches and cameras
- **Digital Citizenship:** The individual or group activity within digital environments
- **E-Learning:** Learning that is facilitated, enhanced or that relies on digital technology. This includes use of the Learning Management System (LMS)
- **Learning Management System (LMS):** is a software application for the administration, documentation, tracking, reporting and delivery of e-learning courses.
- **Social Media** refers to the means of interaction among people in which they create, share and exchange information and ideas in virtual communities and networks (Refer to Social Media Policy).

- **Cyber bullying** is the use of IT equipment that can provide and enable additional routes for those persons intent on bullying. Cyber bullying is covered in our Anti-Bullying Policy, Behaviour Management Policy and Safeguarding and Child Protection Policy.
- **Electronic Communication** refers to all internet based communication between staff and a parent/guardian or a student or ex-student.
- **Extremism** is defined as vocal or active opposition to fundamental values of our society, including democracy, the rule of the law, individual liberty and mutual respect and tolerance of different faiths and beliefs.
- **Radicalisation** is defined as the act or process of encouraging extremist views or actions in others, including forms of extremism leading to terrorism..

7.0 AUDIT AND ASSURANCE

Element to be monitored	Lead	Tool	Freq	Reporting Arrangements	Acting on Recommendations and Lead(S)	Change in Practice and Lessons to be shared

8.0 APPENDICES

Appendix 1: ICT and E-Safety Student User Agreement – School Devices

Appendix 2: ICT and E-Safety Student User Agreement – E-Mail

Appendix 3: ICT and E-Safety Student User Agreement – School ICT

Appendix 4: ICT and E-Safety Parent Agreement

Appendix 5: School ICT Abuse – Behaviour Management guidelines

Appendix 6: ICT Acceptable Use Agreement – Staff, Trustees, Volunteers and Visitors

Appendix 7: Incident Reporting Log

Appendix 8: E-Safety Incident Form

Appendix 9: E-Safety Poster covering E-Safety Rules and details of the e-safety coordinator

Appendix 10: OneSchool Global Online Policy