CANSFIELD

ACHIEVING EXCELLENCE TOGETHER

E-Safety Policy

Approval Date	23rd September 2021
Policy Review Date	September 2022
Chair of Governors	
Headteacher	

1. Purpose

All users need to be aware of the range of risks associated with the use of internet technologies and that some have a minimum age, usually 13 years.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting / Streaming
- Music Downloading / Streaming
- Gaming
- Mobile / Smart phones with text, video and / or web functionality
- Tablets and other mobile devices with web functionality

At Cansfield, we understand the responsibility to educate our pupils on eSafety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Schools hold personal data on learners, staff and other people to help them conduct their day to day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage their reputation.

This policy is inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, smartphones, tablets, webcams, whiteboards, digital video equipment, etc) and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, smartphones and portable media players, etc 'Bring Your Own Device' (BYOD)).

2. Who is the Policy for?

Everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling are made aware of the risks and threats and how to minimise them.

3. Monitoring

Authorised ICT staff may inspect any ICT equipment owned or leased by the school at any time without prior notice. ICT authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, files, emails, instant messaging, computer or internet / intranet use and any other electronic communications (data, voice or image) involving its employees or contractors, without consent, to the extent permitted by the 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 2018, or to prevent or detect crime.

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

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act 2018, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

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

4. Breaches and Incident Reporting

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

Any policy breach is grounds for disciplinary action in accordance with the school's disciplinary procedures. Policy breaches may also lead to criminal or civil proceedings. Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the eSafety Coordinator. Additionally, all security breaches, lost / stolen equipment or data (including passwords), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the eSafety Coordinator.

Please refer to the section below on Incident Reporting, eSafety Incident Log and Infringements.

5. Acceptable Use Policies

AUPs for pupils, staff and Governors are included as appendices at the end of this document.

6. Malware

We use ESET DESlock+ encryption for workstations which may contain sensitive information, i.e. admin workstations where users may require more permissions for bespoke software. Teacher and pupil workstations do not store user information, when the user logs on their account it pulls a mandatory profile down from the server which they cannot save information to and when they log off it deletes profile from the workstation. ESET DESlock+ encrypts the whole harddisk and only the user who is authorised can load the operating system.

We also use ESET Anitvirus with Ransomware protection on all our workstations which monitors activity on workstations and removable devices.

All files downloaded from the internet or received via email must be checked for any viruses using school provided anti-virus software before using them. All portable items, e.g., portable hard drives / USB memory sticks are not permitted

Never interfere with any anti-virus software installed on school ICT equipment that you use. If your machine is not routinely connected to the school network, you must make provision for regular virus updates through IT services.

If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact the IT team immediately, who will advise you what actions to take and be responsible for advising others that need to know.

Never open an email attachment unless you are sure of its origin – even if it looks plausible. If in doubt: delete. Genuine emails can always be resent.

Signs of possible malware infection include:

- Browser pop-ups.
- Redirected home page or search pages (i.e. not what you are used to).
- Sudden, abnormally poor performance (although this may be caused by a number of factors).

- Alarming warnings from software you have not come across before.

If you are in doubt, speak to a colleague or member of the IT team.

In the event of a suspected virus or other malware infection, the following procedure should be followed:

- Immediately notify the IT Technician of the suspected incident.
- Switch off the equipment and, where practical, warn other users of the possible issue.
- Remove any writable, removable media from the machine and pass this to the IT Technician.

The IT Technician will then:

- Isolate the machine and removable media from the network.
- Run an updated, stand-alone virus removal tool on the suspected machine and media.
- Verify the state of virus protection on the main servers.
- Check the state of the infection on the suspect hardware and either:
    - Return it to the network / user if virus removal has been successful.
    - Re-install / re-image / re-format the device if the removal cannot be confirmed.

7. Email

The use of email is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private – Freedom of Information and Subject Access Requests may include email trails, for instance. Educationally, email can offer significant benefits, for instance direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an email in relation to their age and intended recipient.

7.1 Managing Email

The school may give all staff (and pupils) their own email account to use for all school business as a work based tool. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.

- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. The school email account should be the account that is used for all school business.
- Staff are forced to change their passwords every 90 days, their new password must be a minimum length of 8 characters with at least 1 number, uppercase and / or special character.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses. Staff should never use pupils' personal email addresses under any circumstances.
- All emails should be written and checked carefully before sending, in the same way as a letter written on headed paper.
- All pupil email users are expected to adhere to the generally accepted rules of etiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in email communication, nor arrange to meet anyone without specific permission.
- Pupils must immediately tell a member of staff if they receive an offensive email.
- Staff must inform the eSafety Coordinator if they receive an offensive email.
- Pupils are introduced to email as part of the Computing Scheme of Work.
- However you access your school email (whether directly, through webmail when away from the office or on non-school hardware) all the school email policies apply.

7.2 Sending Emails

- Email is an insecure medium. It should not be used for sending personally identifiable or sensitive information (i.e. anything classified as 'Protect' or 'Restricted' in accordance with the Data Protection Policy).
- If you need to send such information within your school, please store the information on the network and simply indicate to the recipient where the information may be found. If you need to send such information to another email domain, please check with the IT Technician for advice. Always check the recipient prior to sending.
- Use your own school email account so that you are clearly identified as the originator of a message.
- Keep the number and relevance of email recipients, particularly those being copied, to the minimum necessary and appropriate.
- Emails containing sensitive information must be encrypted, this can be achieved when composing an email by clicking on the 3 dots … next to where it states *discard* and select encrypt. The recipient will receive an email informing them that they have received an encrypted email. It will include instructions on how to open the email.
- Do not send or forward attachments unnecessarily. Whenever possible, send the location on a shared drive / online folder rather than sending attachments.
- School email is not for personal use and will no longer be available once you leave the school's employment.

7.3 Receiving Emails

- Check your email regularly.
- Activate your 'out-of-office' notification when away for extended periods.
- Never open attachments or click on links from an untrusted source.
- If in doubt: delete.

7.4 Retention of Emails

The Cansfield Data Retention Policy applies to Exchange email, SharePoint sites, OneDrive accounts and Office 365 groups. Information is retained for 3 years after which point it is deleted, when content is subject to the Data Retention Policy, people can continue to edit and work with the content as if nothing's changed because the content is retained in place, in its original location. But if someone edits or deletes content that is subject to the policy, a copy is saved to a secure location where it is retained while the policy is in effect

8. Roles and Responsibilities

The Headteacher and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The school have nominated a named eSafety Manager and an eSafety Coordinator (see below). There is also a nominated eSafety Governor. All members of the school community must be made aware of who holds this post. It is the role of the eSafety Coordinator to keep abreast of current issues and guidance through organisations such as the LA, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and Governors are updated by the eSafety Coordinator and all Governors have an understanding of the issues and strategies at the school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, Governors, visitors and pupils, is to protect the interests and safety of the whole community.

Key staff responsibilities:

Role	Staff member
eSafety Coordinator	Mr P Swain
eSafety Manager	Mrs D Sutch
IT Technician	Mr P Dwyer

9. eSafety Skills Development for Staff

- Staff must receive regular information and training on eSafety issues in the form of INSET training and updates, together with this eSafety Policy.
- New staff receive information on the school's acceptable use policy as part of their induction.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of eSafety and know what to do in the event of misuse of technology by any member of the school community.
- All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas.

10. Managing the School eSafety Messages

- Endeavour to embed eSafety messages across the curriculum whenever the internet and / or related technologies are used.
- The eSafety policy should be introduced to the pupils at the start of each school year.

11. Incident Reporting, eSafety Incident Log and Infringements

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's eSafety Coordinator. Additionally, all security breaches, lost / stolen equipment or data, virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must also be reported.

11.1 eSafety Incident Log

Any incidents should be reported to and recorded by the eSafety Coordinator in the eSafety log, stored securely in a documented location on the school's network – the layout of which is presented below:

Date & Time	Name of pupil or staff member	Gender	Room and computer or device identifier	Details of incident (including evidence)	Actions and reasons

12. Misuse and Infringements

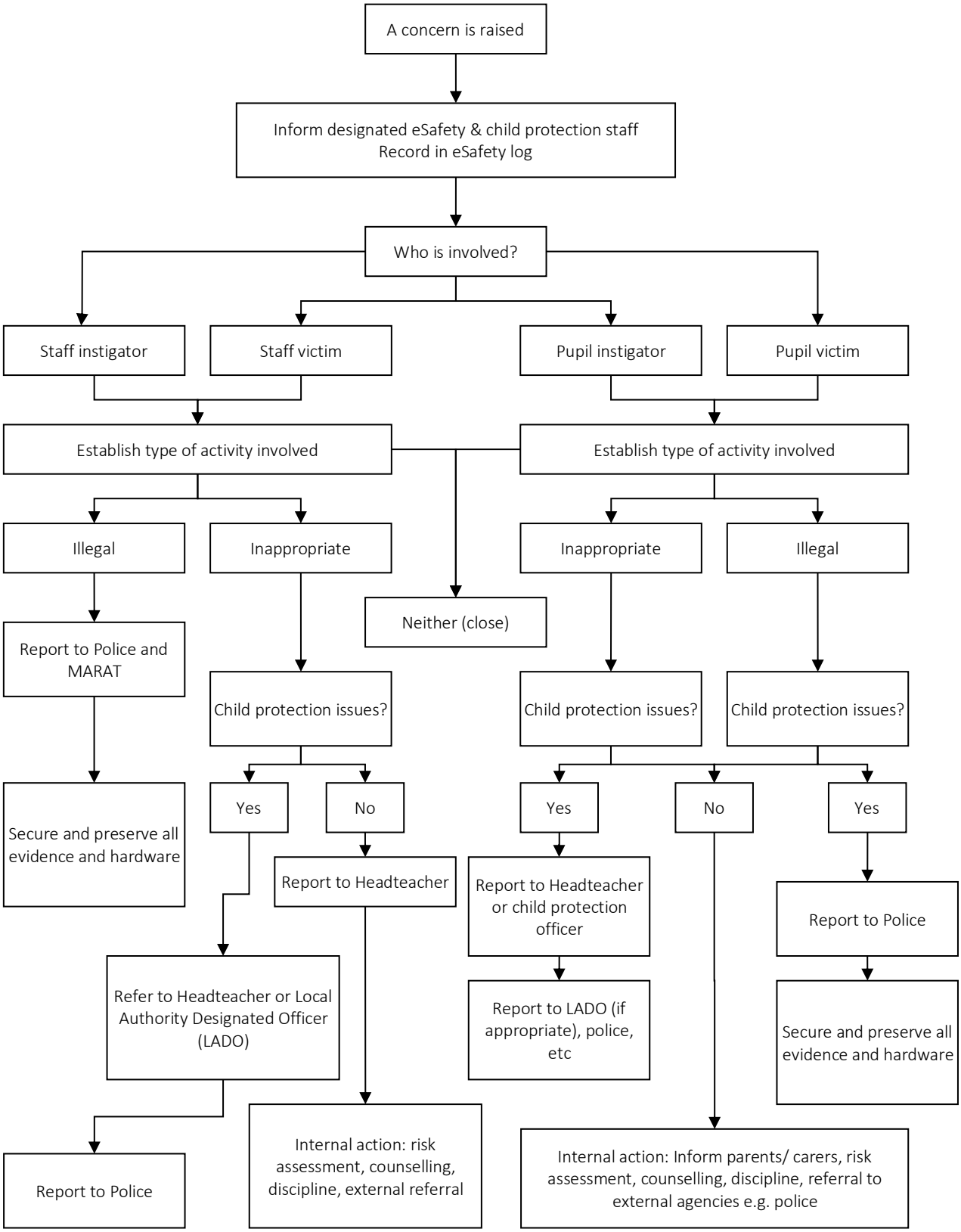
12.1 Complaints

Complaints and / or issues relating to eSafety should be made to the eSafety Coordinator. Incidents should be logged and the flowchart (see below) should be followed.

12.2 Inappropriate Material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the eSafety Coordinator.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the eSafety Coordinator, depending on the seriousness of the offence; investigation by the Headteacher, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see below).

12.3 Flowchart for Managing an eSafety Incident



13. Internet Access

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people.

13.1 Managing the Internet

- The school will provide pupils and staff with supervised access to internet resources (where reasonable) through the school's fixed and mobile internet connectivity.
- Staff must preview any recommended sites or online systems before use.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or software from other sources.
- All users must observe copyright of materials from electronic resources – information made available online cannot be assumed copyright free.

13.2 Internet Use

- You must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise the intended restricted audience.
- Do not reveal names of colleagues, pupils or others, or any other confidential information acquired through your job on any social networking site or other online system.
- Online gambling or gaming is not permitted.
- Please check with the eSafety Manager before downloading apps for use in school, by staff, pupils or parents so that compliance with GDPR and the Data Protection Act 2018 can be checked.

13.3. Prevent Duty

Guidance on the Counter-Terrorism and Security Act 2015 – to have due regard to the need to prevent people from being drawn into terrorism (a.k.a. 'Prevent') – explicitly states that: 'Specified authorities will be expected to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering.'

While this duty does not confer new functions on any specified authority (i.e. Cansfield), 'the term 'due regard' as used in the Act means that the authorities should place an appropriate amount of weight on the need to prevent people being drawn into terrorism when they consider all the other factors relevant to how they carry out their usual functions'. Hence there is an expectation to pay specific attention to the filtering of sites which could be seen as likely to draw young people into terrorism, or to extremist ideologies.

Where a pupil is found to be accessing such material without legitimate purpose (e.g. as part of a Citizenship assignment), it should be treated as a safeguarding issue.

13.4 Social Media (and other 'Web 2.0' Technology)

Online technology, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However, it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

13.5 Pupils

- All pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are.
- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- Pupils are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile / home phone numbers, school details, IM / email address, specific hobbies / interests).
- Our pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts online.
- Our pupils are asked to report anything which causes them concern (e.g. incidents of bullying, inappropriate requests for contact) to the school or a trusted adult.

- Pupils must not use public social media for school business without the knowledge of the eSafety Coordinator.
- Cyberbullying (along with all forms of bullying) will not be tolerated in school.
- There will be clear procedures in place to support anyone affected by cyberbullying.
- All incidents of cyberbullying reported to the school will be recorded.
- There are procedures in place to investigate incidents or allegations of cyberbullying.
- Pupils, staff and parents / carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify the bully, where appropriate, such as examining system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Sanctions for those involved in cyberbullying may include:
    - The bully will be asked to remove any material deemed to be inappropriate or offensive.
    - A service provider may be contacted to remove content.
    - Internet access may be suspended at school for the user for a period of time.
    - Parent / carers may be informed.
    - The Police will be contacted if a criminal offence is suspected.

13.6 Staff

Staff should be aware of the Data Protection Act 2018 and implications redarding GDPR when considering creating blogs, wikis or other online systems in order to communicate with pupils and are advised to check with the eSafety Manager. We do not permit any use of Facebook or other social media sites to engage with pupils for social purposes but may allow access to such sites by individual approval and agreement with the eSafety Coordinator (with controls introduced to minimise opportunity for abuse) for educational purposes (within the terms set out by the site which may prohibit such use).

- Do not talk about your professional role in any capacity when using social media.
- The eSafety Coordinator must be informed of any blogs created or endorsed by members of staff for use with pupils. These blogs must either require passwords or moderation before posts can be added.
- Staff must ensure that all posts made on social networking sites, whether inside or outside of the school, reflect the high professional standards expected by Cansfield High School.
- Staff must not use social networking sites as a forum to make derogatory comments which could bring the school into disrepute, including comments about members of the school community.
- Staff are expected to demonstrate honesty and integrity and uphold public trust and confidence in respect of anything placed on social networking websites.
- Staff must ensure that any content shared on any social networking website, at any time, would be deemed as appropriate. Staff are personally responsible for ensuring that any privacy settings meet this requirement.
- Staff must ensure appropriate language is used at all times for any comments placed on social networking sites.
- Staff must ensure that any communication and / or images, at any time, could not be deemed as defamatory or in breach of any relevant legislation.
- Friend requests (or equivalent) from pupils must be declined.
- Staff must not establish contact with pupils through their personal social networking sites, or any other means of electronic communication (including personal email or telephone). All contact with pupils must be directly concerned with the pupils' education.
- Staff should refrain from contacting former pupils via personal email or social media.
- Staff should exercise caution in the use of social media where their 'digital social circle' (i.e. friends, followers, etc) may include other members of the school community, particularly parents. Be aware that this may lead to indirect communication with pupils – it may be prudent to 'unfriend' such individuals or at least inform a line manager via email of any such connections.
- Staff must not publish photographs, videos or any other types of image of pupils or their families on personal social networking accounts, or school accounts where permission for publication of images has not been granted.

13.7 Parental Involvement

We believe that it is essential for parents / carers to be fully involved with promoting eSafety both in and outside of school and also to be aware of their responsibilities. We regularly consult and discuss eSafety with parents / carers and seek to promote a wide understanding of the benefits related to ICT and associated risks.

Parents / carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school; they are required to make a decision as to whether they consent to images of their child being taken / used in the public domain (e.g. on school website). The school disseminates information to parents relating to eSafety where appropriate in the form of:

- Information evenings
- Website postings
- Email
- Twitter
- Letters

14. ICT Equipment including Portable and Mobile Equipment and Removable Media

14.1 School owned ICT equipment

- As a user of IT, you are responsible for any activity undertaken on the school's ICT equipment provided to you.
- The school logs IT equipment issued to staff and record serial numbers as part of the school's asset register.
- Personal or sensitive data must not be stored on the local drives of desktop PCs. If it is necessary to do so the local drive must be encrypted.
- A time locking screensaver is applied to all machines. Please lock your machine when you move away from it – even momentarily.
- Privately owned ICT equipment may only be connected to the Wi-Fi network – contact the IT Technician for further guidance.
- On termination of employment, resignation or transfer, return all IT equipment to your line manager. You must also notify the IT Technician so that accounts can be disabled.
- All IT equipment allocated to staff must be authorised by the appropriate line manager.

Authorising Managers are responsible for:

- Liaising with the IT Technician to ensure compatibility.
- Maintaining control of the allocation and transfer within their area.
- Recovering and returning equipment when no longer needed.
- All redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA) 2018.

14.2 Portable and Mobile ICT Equipment

This section covers such items as laptops, mobile phones, tablets and removable data storage devices. Please refer to the Data Protection Policy when considering storing or transferring personal or sensitive data.

- All activities carried out on school systems and hardware will be monitored in accordance with the general policy.
- Ensure portable and mobile IT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades.
- The installation of any applications or software packages must be authorised by the IT Technician, fully licensed and only carried out by the IT Technician.
- In areas where there are likely to be members of the general public, portable or mobile IT equipment must not be left unattended and, wherever possible, must be kept out of sight.
- Portable equipment must be transported in its protective case if supplied.

14.2.1 Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for pupils. Many existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and smartphones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse

associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed.

14.2.2 Bring Your Own Device (BYOD)

- The school allows staff to bring in personal mobile phones and devices for their own use.
- Pupils are allowed to bring personal mobile devices / phones to the school but must not use them for personal purposes within lesson time.
- It is the responsibility of the device owner to ensure the device is suitably charged and in good working order.
- Where devices are required for lessons, the school will make devices available for loan as an alternative to BYOD.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate communication between any members of the school community is not allowed.
- Permission must be sought before any video, image or sound recordings are made on these devices of any member of the school community.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.
- Devices used in lessons must be connected to the school's own filtered Wi-Fi in such a way that the user of the device may be identified so that appropriate filtering policy may be applied and monitored. The school cannot be responsible for websites or services accessed through other forms of mobile internet access (e.g. 3G / 4G connections).
- Mobile internet sharing / hotspots should be disabled as they can interfere with the school's own Wi-Fi connection.

14.2.3 Pupil Use of Mobile Phones

Mobile phones and other personal devices such as tablets, smartphones, etc. are considered to be an everyday item in today's society and pupils and staff may own and use such devices to regularly get online. Mobile phones and other internet enabled devices can be used to communicate in a variety of ways with texting, camera phones and internet access all common features. Mobile phones can present a number of problems when not used appropriately:

- Their use can render pupils or staff subject to cyberbullying.
- Mobile phones with integrated cameras could lead to child protection, bullying and data protection issues with regard to inappropriate capture, use or distribution of images of pupils or staff.
- Internet access on phones and personal devices can allow pupils to bypass school security settings and filtering.
- They can undermine classroom discipline as they can be used on 'silent' mode.
- They are valuable items which may be stolen or damaged.

Due to the widespread use of personal devices it is essential that pupil use of mobile phones does not impede teaching, learning and good order in classrooms. Staff are given clear boundaries on professional and classroom use.

- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school's Behaviour Policy.
- School staff may confiscate a phone or device if they believe it is being used to contravene the schools' Behaviour Policy and Anti-Bullying Policy. The phone or device might be searched by a member of the Senior Leadership Team with the consent of the pupil or parent / carer. If there is suspicion that the material on the mobile may provide evidence relating to a criminal offence the phone will be handed over to the police for further investigation.
- Mobile phones and personal devices will only be used at break and lunchtime in the canteen or drop-in area for each year group.
- They should be switched off at all times outside agreed 'phone zones'.
- The Bluetooth function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.

- Electronic devices of all kinds that are brought in to school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.
- Mobile phones and personal devices are not permitted to be used in certain areas within the school site such as changing rooms, toilets and swimming pools.

14.2.4 School Provided Mobile Devices (including Phones)

- Mobile Device Management software should be installed onto all school owned portable devices for management and monitoring.
- The sending of inappropriate communication between any members of the school community is not allowed.
- Permission must be sought before any video, image or sound recordings are made on the devices of any member of the school community.
- Where the school provides mobile technologies such as phones, laptops and PDAs for offsite visits and trips, only these devices should be used.

15. Systems Access

- You are responsible for all activity on school systems carried out under any access/account rights assigned to you, whether accessed via school IT equipment or your own hardware.
- All access to IT systems and the internet must be via approved systems which provide appropriate management, filtering and security.
- Do not allow any unauthorised person to use school IT facilities and services that have been provided to you.
- Ensure that you logoff from the PC completely when you are going to be away from the computer for a longer period of time.
- Do not introduce or propagate viruses.
- It is imperative that you do not access, load, store, post or send from school ICT any material that is, or may be considered to be, illegal, offensive, libellous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the school or may bring the school in to disrepute. This includes, but is not limited to, jokes, chain letters, files, emails, clips or images that are not part of the school's business activities; sexual comments or images, nudity, racial slurs, gender specific comments, or anything that would offend someone on the basis of their age, sexual orientation, religious or political beliefs, national origin, or disability (in accordance with the Sex Discrimination Act, the Race Relations Act and the Disability Discrimination Act).

16. Telephone Services

- You may make or receive personal telephone calls provided:
    - They are infrequent, kept as brief as possible and do not cause annoyance to others.
    - They are not for profit or to premium rate services.
    - They conform to this and other relevant school policies.
- School telephones are provided specifically for school business purposes and personal usage is a privilege that will be withdrawn if abused.
- Ensure that your incoming telephone calls can be handled at all times.

17. Mobile Phones and other School Provided Portable Devices

- You are responsible for the security of your school mobile phone or device.
- Report the loss or theft of any school mobile phone or device immediately – the school remains responsible for all call costs until the phone is reported lost or stolen.
- You must read and understand the user instructions and safety points relating to the use of your school mobile phone prior to using it.
- School SIM cards must only be used in school provided mobile phones.
- School mobile phones may be barred from calling premium rate numbers and any numbers outside of the UK.
- You must not send text messages to premium rate services.
- You must reimburse the school for the cost of any personal use of your school mobile phone. This includes call charges incurred for incoming calls whilst abroad.

18. Infrastructure

- School has a network and device monitoring solution called Impero Education Pro, with keyword detection, real-time monitoring, access management, and activity logs and incident handling, which helps teachers and school administrators keep pupils safe.
- Fixed internet access is controlled via the Smoothwall UTM1000 Device, which provides web filtering plus firewall protection with real-time monitoring to keep our network, staff and pupils safe.
- BYOD internet access in controlled through an onsite web filter – note that the filtering rules of these two systems may not precisely coincide.
- Staff and pupils are aware that school-based computer and internet activity can be monitored and explored further if required.
- If staff or pupils discover an unsuitable site, the screen must be switched off / closed and the incident reported immediately to the eSafety Coordinator or teacher as appropriate.
- It is the responsibility of the school, by delegation to the Network Manager, to ensure that anti-virus protection is installed and kept up to date on all school machines.
- Pupils and staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility, nor the IT Technician's, to install or maintain virus protection on personal systems. Windows 10 comes with in-built security 'Windows Defender'.
- Pupils and staff are not permitted to download programs or files on school-based technologies without seeking prior permission from the Network Manager.
- If there are any issues related to viruses or anti-virus software, the IT team should be informed immediately.
- If you require a site that is normally blocked to pupils open in an IT suite or on mobile internet devices this must be raised with the IT Technician in a timely manner (i.e. with at least 24 hours' notice).

19. Appendix 1: Acceptable Use Agreement: Pupils

- I will only use ICT systems in the school, including the internet, email, digital video, mobile technologies, etc. for school purposes.
- I will not download or install software on school equipment without approval from the IT Technician.
- I will only log on to the school network or other areas or platforms with my own user name and password.
- I will follow the school's ICT security system, password recommendations and not reveal my passwords to anyone and change them as required.
- I will make sure that all ICT communications with pupils, staff or others is responsible and sensible.
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to a member of staff.
- I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone unless this is part of a school project approved by my teacher.
- Images of pupils and / or staff will only be taken, stored and used for school purposes in line with school policy and not be distributed outside the school network without the permission of the eSafety Coordinator. I will not take recordings, images or videos of other members of the school community (including other pupils and school staff) without their knowledge or consent.
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, pupils or others distress or bring into disrepute. This includes the use of social media sites (including Facebook), blogs and microblogging sites (such as Twitter) and media sharing sites and apps (such as Snapchat).
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community both inside and outside of the school.
- I will respect the privacy and ownership of others' work online at all times.
- I will not attempt to bypass the internet filtering system.
- I understand that all my use of the internet and other technologies can be monitored and logged and can be made available to my teachers.
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent / carer may be contacted.
- If I do not have access to an internet connection or other required technology to complete a piece of work, I will do the work on the computers at the school or print the work at the school and complete on paper.

Pupils are expected to read and discuss this agreement with their parent or carer and then to sign and follow the terms of the agreement. Any concerns or explanation can be discussed with their form teacher.

Please return this form to school.

Pupil and Parent / Carer signature

We have discussed this document and ……(pupil name) agrees to follow the eSafety rules and to support the safe and responsible use of ICT at Cansfield High School. I am aware that my child may be required to access approved online resources or social media as part of his or her homework but that offline alternatives will be made available where necessary.

Parent / Carer Signature …….

20. Appendix 2: Acceptable Use Agreement: Staff, Governors and Visitors

ICT (including data) and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. This document is intended as guidance and recommendations for the protection of all members of the school community. Any concerns or clarification should be discussed with the school eSafety Coordinator.

- I will only use the school's email / internet / learning platform and any related technologies for professional purposes or for uses deemed reasonable by the Headteacher.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not use my school email account for personal use (e.g. online shopping sites, mailing lists, etc).
- I will not forward confidential school emails to non-school accounts, or access school email by any insecure method (usual web access *is* considered secure). I will report the loss of any mobile device with access to school email to the IT Technician immediately so it may be wiped remotely.
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
- If I use social media I am aware of the potential risks and the recommendations contained within the eSafety and associated policies – and will act in accordance with the Data Protection Act 2018
- I will use the approved, secure email system(s) for any school business.
- If I intend to use my own devices for school use (including email) I will comply with the BYOD section of the Data Protection Policy.
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school or accessed remotely.
- I will not store, transfer or transmit by email attachment or other insecure method any personally identifiable information (including class lists). I understand that this prohibits the use of ~~unencrypted memory sticks or other~~ portable media for transferring data about specific, identifiable (i.e. named) pupils, or storing any such data on computers outside of school.
- I will not install any hardware or software without permission of the IT Technician.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory unless reasonably part of lesson content.
- I will refer to the advice as per the Data Protection Policy for the taking and processing of images of pupils.
- I understand that all my use of the internet and other related technologies can be monitored and logged and can be made available, on request, to my line manager or eSafety Coordinator.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute, in accordance with the Teaching (or other professional) Standards where appropriate.
- I will support and promote the school's e-Safety Policy and Data Protection Policy and help pupils to be safe and responsible in their use of ICT and related technologies.

User Signature

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the School.

Signature ……. Date …….

Full Name …….. (BLOCK CAPITALS)