Digital Learning and Safety Policy

NGHS A007

Contents:

Document Control	
Title	A007 Digital learning and Safety Policy
Date	June 2020
Supersedes	Digital Learning and E-Safety Policy September 2018
Amendments	
Related Policies/Guidance	Safeguarding Policy, Data Protection Policy
Review	June 2022
Author	P Fearon
Date consultation completed	18-9-2020
Date adopted by Trust Board	

Prospere Learning Trust *(Previously CHS Learning Trust and Piper Hill Learning Trust)* is a Multi Academy Trust. Registered in England and Wales - number 10872612
Registered Office: Piper Hill High School, Firbank Road, Wythenshawe, M23 2YS

The Prospere Learning Trust has a number of Trust-wide policies which are adopted by all schools/academies in the Trust to ensure an equitable and consistent delivery of provision.

The Trust Board has responsibility for the operation of all schools/academies and the outcomes of all students however responsibility is delegated to the Local Governing Body of each school via the Scheme of Delegation.

Within our policies reference to:

- Governing Body / Governors relates to the members of the Local Governing Body representing the Trust Board.
- School includes reference to school, academy or free school unless otherwise stated.
- Headteacher includes reference to Headteacher, Principal or Head of School of the school, academy or free school.

1. Introduction:

1.1. This policy has been formulated to ensure that there are effective processes and procedures in place within Newall Green High School to facilitate safe, secure and high quality access to digital technology and the wealth of information that is now available through digital systems.

1.2. This policy deals with the use of ICT systems at Newall Green High School outlined below, and applies to all ICT 'Users'.

1.3. The term 'User' applies to any school employee, student or other authorised person (e.g. parents, volunteers, staff from external agencies, partner organisations & community organisations) who uses the school's ICT systems and/or data.

1.4. For the purposes of policy and practice within school this document is intended to cover all aspects of ICT/digital technology use and the use of information systems to store and retrieve information.

1.5. 'ICT' (or 'ICT system') means any device/system/network for storing, processing, and accessing data/information. (For example: server, personal computer, laptop, tablet portable device, workstation, MIS system, mobile phone, generic music/video player (i.e. iPod), messaging system or any other similar device or system).

1.6. 'Digital Resources' (or 'ICT resources') means any piece of hardware/software/storage equipment (E.g. the hardware above, printers, cameras, digital recorders, storage devices, hard drives, pen drives, school hosted software, external hosted software/information sources, the school's Virtual Learning Environment, the school's website, the internet, communication facilities both internal and external.

1.7. 'ICT data' means any information stored and processed by ICT and includes programs, text, pictures and sound whether internally or externally hosted or processed.

1.8. This policy applies equally to use of school equipment both in and outside of school and to the use of Users personal digital equipment on the school premises

2. The Legal Framework:

2.1. The responsibilities referred to in this document recognise the requirements of the current legislation relating to the use of ICT systems, which comprise principally of the following Acts:

2.2. Data Protection Acts 1984 & 1998:

- The Data Protection Act exists to regulate the use of computerised information about living individuals. It is important that all users of personal data are aware of, and are reminded periodically of, the requirements of the act and, in particular, the limitations on the storage and disclosure of information.
- The Trust's Data Protection Policy (D001) provides staff with further guidance on this issue.

2.3. Computer Misuse Act 1990:

Under the Computer Misuse Act 1990 the following are criminal offences, if undertaken intentionally;

- Unauthorised access to a computer system or data;
- Unauthorised access preparatory to another criminal action;
- Unauthorised modification of a computer system or data.

2.4. Copyright, Designs and Patents Act 1988:

The Copyright, Designs and Patents Act 1988 provides the legal basis for the protection of intellectual property which includes literary, dramatic, musical and artistic works. The definition of "literary work" covers computer programs and data.

- All copying of software is forbidden by the Act unless it is in accordance with the provisions of the Act and in compliance with the terms and conditions of the respective licence or contract.

2.5. Safeguarding Legislation- Education Act 2002:

- Under the Education Act 2002 schools have a duty to safeguard and promote the welfare of their students and, in accordance with guidance set out in 'Working Together to Safeguard Children' (2013) and 'Keeping Children Safe in School'(2014), Newall Green High School will work in partnership with other organisations where appropriate to identify any concerns about child welfare and take action to address them.

2.6. Counter Terrorism and Security Act 2015 (The Prevent Duty)

The above act contains a duty on specified authorities to have due regard to the need to prevent people from being drawn into terrorism.

2.7. It is important that all Users are aware that any infringement of the provisions of current legislation may result in disciplinary, civil and/or criminal action

3. Key Roles and Responsibilities:

3.1. The Governing Body of the school will ensure that:

- The school effectively uses ICT and digital technology to enhance the learning experiences of students at Newall Green High School.
- The school complies with the legislative requirements relating to the use of ICT systems and for disseminating policy on digital safety, ICT security and other ICT related matters.
- Its employees act in a lawful manner, making appropriate use of school technologies for approved purposes only.
- There is a Senior Leader who is designated to take the lead on Digital Learning and Safety within the school.
- Procedures are in place for dealing with breaches of Digital safety and security and are in line with best practice guidelines.
- All Users have access to appropriate ICT training.

3.2. The Headteacher of the school will ensure that:

- The legislative requirements relating to the use of ICT systems are met.
- The school's ICT security and digital safety procedures are robust and kept under regular review and scrutiny.
- Day to day functions for the safe operation of the school's ICT systems are appropriately delegated as required.
- A Designated Senior Leader for Digital Learning and Safety is identified, receives appropriate on- going training/support and works closely with the Designated Person for Safeguarding.
- A commitment to digital learning and safety is an integral part of the safer recruitment and selection process of staff and volunteers.
- Sufficient resources are allocated each year to ensure the security and integrity of the school's ICT systems to enable Users to comply fully with legal requirements.
- Users will be made aware of the value and importance of ICT systems and data, particularly data of a confidential or sensitive nature, and be made aware of their personal responsibilities for ICT

security. Adequate procedures are established in respect of the ICT security implications of personnel changes. Suitable measures should be applied that provide for continuity of ICT security when staff vacate or occupy a post.

- The requirements of the Data Protection Act 1998 are complied with fully by the school (see Trust Data Protection Policy (D001)
- Details of any suspected or actual breach of ICT security are recorded and made available to the Audit committee. (The Headteacher must advise the Audit Committee and Academy Trust of any suspected or actual breach of ICT security pertaining to financial irregularity.)
- If there is reason to believe that any ICT equipment has been misused, they will consult the school's HR provider and ICT provider for advice without delay. The school's HR provider will agree with the Headteacher an appropriate strategy for the investigation of the allegations. Incidents will be investigated in a timely manner in accordance with agreed procedures.
- An appropriate management system is implemented detailing security access rights for all Users.
- A record is kept of students whose parents/carers have specifically requested that their child be denied internet or e-mail access and ensure that access rights and arrangements are regularly checked to ensure that parent's wishes are being adhered to.
- There is close liaison with the SLT member responsible for Data Protection to ensure that the school's ICT systems operate within the constraints of the school's data protection policy.

3.3 The SLT member with responsibility for Digital Learning & Digital Safety will:

- Be responsible for digital learning across the school, including the development of cross- curricular ICT.
- Monitor the curriculum and report to the Headteacher termly on progress with regard to the school's development plan and developments in digital learning.
- Ensure that the planning and development of digital learning across the school is in line with current educational developments nationally.
- Attend appropriate Continued Professional Development (CPD) and provide support and training for all Users on digital learning and safety.
- Be responsible for the development and safe operation of the school's Virtual Learning Environment (VLE).
- Act as the first point of contact with regards to breaches in digital safety and security.
- Ensure that all SLT members, the teaching and non-teaching staff understand and can apply the Digital Safety Issues SOP.
- Liaise with the Designated Person for Safeguarding as appropriate.
- Ensure that all Users have read and understand the school's Digital Learning and Safety Policy and agree to abide by it.
- Ensure that all Users understand that misuse of ICT systems may lead to disciplinary action and possible dismissal.
- Advise Users on managing digital equipment and software to enhance learning in the curriculum.
- Promote equal opportunities for computer usage and fairness of distribution of digital resources.
- Monitor the level of access to computers in the home environment to ensure no students are unduly disadvantaged.

3.4 The Trust ICT Network Manager will ensure that:

- The school's network and ICT systems including all hardware and software is managed and operated effectively to meet the needs and requirements of all Users.
- The school's partners / providers deliver effective day to day operation of all ICT systems across the school in line with contracts or SLAs.
- There is an up to date and accurate asset inventory of the school's ICT/digital equipment, systems and software.
- Adequate controls and access arrangements are in place for all ICT/digital assets and for defining and documenting the requisite level of protection and security required.
- Day to day ICT administrative functions are performed such as the practical aspects of ICT protection and security, maintaining the integrity of data, producing back-up copies of data and protecting the physical access and security of systems and data.
- ICT security is maintained across the network on a day-to-day basis and that all security procedures are regularly monitored to ensure the safe operation of the school's systems.
- There is a robust system in place to ensure appropriate online filters and monitoring systems are in place to protect children from harmful online material, including but not limited to: pornography, self-harm sites and extremist material such as Daesh propaganda and advice on how to travel to Syria.
- Production of a regular report for the Headteacher on internet activity/usage by students and active sharing of any concerns with the Safeguarding team.
- Periodic audits of software held on ICT equipment are undertaken and appropriate licences are in place for all software.
- Any suspected or actual breach of ICT security occurring within the school is reported to the Headteacher or Chair of Governors.

3.5 The School's ICT Technicians will ensure that:

- The school's ICT systems are effectively managed and maintained on a day to day basis.
- The school's hardware and software are well maintained and operational at all times.
- Repairs and maintenance are undertaken swiftly and effectively using approved external providers as appropriate.
- Security systems including Virus Protection and Firewalls across the school's networks are robust, effectively managed, regularly updated and reviewed.
- They maintain an up to date asset register of all digital equipment and software across the school's network.
- They undertake annual checks of the school's software inventory to ensure that valid software licences support all installations.
- The school's ICT systems operate within the constraints of the school's data protection policy.
- There is a robust system for the 'Backup' and 'Disaster Recovery' processes within school which is regularly monitored so that our essential services and facilities are restored as quickly as possible following an ICT system failure.
- The majority of 'Backups' are stored as part of the school's Disaster Recovery (DR) Servers and any 'Backup tapes' (where required) are stored securely in the School's fire resistant safe.
- There is a robust system for the monitoring and supervision of access to the internet from the school site and implement restrictions / lift restrictions as appropriate to ensure that internet access is safe and secure at all times.
- Prior to the transfer or disposal of any ICT equipment any personal data or software is obliterated from the machine or arrange for an authorised organisation to do this on our behalf.

4. <u>Acceptable Use of Digital Technology for Adult Users:</u>

4.1. User Responsibilities and Conduct:

4.1.1. By logging on to the school's ICT systems or using the school's ICT/digital equipment Users agree to abide by the school's Digital Learning and Safety Policy.

4.1.2. It is the duty of all Users to ensure children and young people at Newall Green High School are safe and secure when using our ICT systems.

4.1.3. The benefit of using the Internet is to allow access to world-wide educational resources, and Users must take reasonable precaution to ensure that students only access appropriate material. Staff must ensure that any material viewed is age appropriate.

4.1.4. When Users wish to use internet sites, or material downloaded from the internet, for example clips from 'YouTube', they must have been viewed prior to the lesson to ensure they are fully appropriate for the age range and needs of students.

4.1.5. Users may only use ICT resources to access suitable material – Using ICT to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive is not permitted.

4.1.6. It is possible to access or be directed to unacceptable Internet sites by accident. If Users have accessed unacceptable content or are in receipt of unacceptable material, they should inform their Line Manager or a member of SLT immediately.

4.1.7. All users must understand that deliberate unauthorised use, alteration, or interference with a computer system or its software or data, whether proprietary or written 'in-house', will be regarded as a breach of school policy and subject to disciplinary action. It must also be noted that in some circumstances such a breach may also be a criminal offence.

4.1.8. The school's ICT facilities must not be used in any way that breaks the law or breaches standards detailed in Computer Misuse Act 1990. Such breaches include, but are not limited to:

- making, distributing or using unlicensed software or data;
- making or sending threatening, offensive, or harassing messages, material or communications;
- creating, possessing or distributing obscene material;
- unauthorised private use of the school's computer facilities.

4.1.9. No one may use ICT resources in violation of license agreements, copyrights, contracts or national laws, or the policies, rules or procedures of the school.

4.1.10. All suspected or actual breaches of ICT security shall be reported to the SLT member responsible for Digital Learning and Safety or, in their absence, the Headteacher.

4.1.11. Any faults with the school's ICT system should be reported to the school's ICT Technicians who will take the appropriate course of action.

4.2. System Security:

4.2.1. Users must not share their account details with others for their use, nor utilise another users' account or misrepresent their identity for any reason.

4.2.2. Users must not under any circumstances reveal their password to anyone else and must ensure that their password is a 'strong password' following basic password security at all times.

4.2.3. No User shall access another User's personal electronic documents (including email) without the owner's permission or as allowed by this policy or by law.

4.2.4. Users must not load or download software on any device without the authorisation of the ICT Infrastructure Leader.

4.2.5. Users must get prior permission in writing from the ICT Infrastructure Leader before copying any software.

4.2.6. Users must ensure that for all Master Disks and licences held within Curriculum Areas, a copy is held by the ICT Technical Support team.

4.2.7. Users who have been issued with a digital device (E.g. mobile phone, laptop, iPad) to assist them in their professional duties will be expected to sign for its use on receipt. Staff may take such resources home for work outside of school but must ensure that they use them in line with this policy and ensure the security and confidentiality of any data stored on such devices at all times. Upon leaving employment with the school staff must return such items for them to be re-issued.

4.2.8. Users have the responsibility to take precautions to prevent the initial occurrence and subsequent spreading of a computer virus. No one may knowingly create, install, run, or distribute any malicious code or another destructive program on any ICT resource.

4.2.9. Users must immediately report any instance of suspect or actual computer virus infection to the ICT Technicians who must take appropriate action, including removing the source of infection.

4.2.10. Network connected devices must have school approved anti-virus software installed and activated. Users may not turn off anti-virus software.

4.2.11. No User may knowingly or willingly interfere with the security mechanisms or integrity of ICT resources. No one may use ICT resources to attempt unauthorised use, or interfere with the legitimate use by authorised users, of other computers on internal or external networks. Access to networks will be monitored.

4.3. Data Security:

4.3.1. Users are expected to act in a responsible, ethical and lawful manner with the understanding that school electronic and manual information may be accessible to the public under the Freedom of Information Act 2000.

4.3.2. Users should uphold privacy and confidentiality in accordance with the Data Protection Act 1998. Care must also be taken not to breach another person's copyright, trademark or design, nor to publish any defamatory content.

4.3.3. Users must take care to store sensitive information, e.g. student data safely and to keep it securely protected, on all school systems, including laptops and portable devices.

4.3.4. Users must not send personal data or sensitive and confidential information by unencrypted email to an external recipient.

4.3.5. Data should be only stored and accessed through the school's SIMS systems, the school's internal computer network or the school's VLE. Usually this will mean storing it in appropriate folders in subject server areas.

4.3.6. The principle of 'Data Transfer' in school between users is to 'Direct other users to LOOK' at data rather than sending data to them.

4.3.7. Portable and mobile computer devices such as laptops used to store and process personal data which could cause damage or distress to individuals should be password protected and encrypted.

4.3.8. Whilst staff may use pen drives or portable hard drives CD disks or flash memory devices to transfer files between home and school, files that contains personal data should NOT be stored or transported in this manner. Such storage devices should be encrypted/password protected at all times.

4.3.9. Reasonable care must be taken in the positioning of computer screens, printers or other similar devices so that information stored or being processed cannot be viewed by persons not authorised to know the information.

4.3.10. Users must not leave computers logged-on when unattended.

4.3.11. Disposal of waste ICT media such as print-outs, discs, magnetic tape, hard drives and solid state devices will be made with due regard to the sensitivity of the information they contain. For example, paper will be shredded if any confidential information from it could be derived.

4.4. <u>Personal use and privacy:</u>

4.4.1. In the course of normal operations, digital resources are to be used for business purposes only. The school permits limited personal use of digital resources by authorised users subject to the following limitations:

- Personal use must be in the user's own time and must not impact upon work efficiency or costs.
- The level of use must be reasonable and not detrimental to the main purpose for which the facilities are provided.
- Personal use must not be of a commercial or profit-making nature.
- Personal use must not be of a nature that competes with the business of the school or conflicts with an employee's obligations.
- Personal use must not breach any of the guidance or direction contained in the relevant policies covering professional use of digital technologies.
- In particular, personal use must not involve attempting to access the categories of content which are unlawful, obscene or offensive.

4.4.2. Within the terms of the Data Protection Act 1998, Human Rights Act 1998 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, the school may record or inspect any information transmitted through or stored in its ICT systems including email communications and telephone conversations without notice when:

- There is reasonable cause to believe the user has violated or is violating school policy, guidelines or procedures.
- An account appears to be engaged in unusual or unusually excessive activity.
- It is necessary to do so to protect the integrity, security, or functionality of ICT resources or to protect the school or its partners from liability.
- Establishing the existence of facts relevant to the business.

- Ascertaining or demonstrating standards which ought to be achieved by those using the ICT facilities.
- Preventing or detecting crime.
- Investigating or detecting unauthorised use of ICT facilities.
- Ensuring effective operation of ICT facilities.
- Determining if communications are relevant to the business (for example, in the last resort where an employee is off sick or on holiday and business continuity is threatened).
- It is otherwise permitted or required by law.

4.5. Electronic communication:

4.5.1. Users should not use personal mobiles for texting or phone calls during student contact hours, including lessons and duty times. If there is an emergency and you need to leave your phone on please inform a Senior Leader.

4.5.2. Users must not give their home telephone number or their personal mobile phone number to students or student family members.

4.5.3. Users must not use their personal mobile phones to contact students from the school. They will have access to a school mobile phone where contact with students is necessary. Personal mobile phones must not be used to photograph school activities involving students.

4.5.4. Users must not make use of students' mobile phone numbers either to make or receive phone calls or to send to or receive text messages other than for approved school business using approved school equipment that has been agreed by a Senior Leader.

4.5.5. Users must ensure that they do not have personal contact or communication with students / ex-students under the age of 21 on-line or through other forms of digital communication e.g. Facebook (including mobile phones) and adhere to the guidance outlined in this policy and appropriate safeguarding policies.

4.5.6. Users must use the school e-mail system or school communication accounts if they need to communicate with students about their schoolwork e.g. study leave, course work etc. A designated member of SLT will be responsible for monitoring school communication accounts. Passwords for all accounts must be stored centrally.

4.5.7. If Users are approached online by students at the school they should not enter into contact with them. Such contact must be logged with their SLT line manager, Safeguarding or SLT member responsible for Digital Learning & Safety.

4.5.8. If Users are sent inappropriate material e.g. messages, images or videos, report it immediately to a Senior Leader and safeguarding.

4.5.9. On occasions ex-students may attempt to contact staff, for example to ask for a reference or to engage with our alumni. Any communication with them should be for professional reasons only. Responses should be via the school's email system or communication forums, and Users should copy in line managers to their response. This is to protect all parties.

4.5.10. In school time social networking sites (e.g. Instagram, Facebook and Twitter) should not be accessed by staff unless being used for educational purposes.

4.5.11. If staff access and use social networking/online sites outside of school it is important that they continue to follow this guidance. They should ensure that comments made and activities entered into on line do not endanger their own professionalism or the reputation of the school. Confidentiality about school matters is paramount and should not be discussed in such forums. Improper use of social media, including private social media accounts, could amount to gross misconduct.

4.5.12. Staff using such sites outside of school must not add current or past students as friends. The only exception to this rule ***is*** where the pupil is a member of the staff's family ***provided agreed protocols are followed and the family relationship has been identified to and acknowledged by the Headteacher.*** In cases where a pupil is a family member, staff must be aware that if the family relationship has not been identified and acknowledged by the school, contact through social networking or social media will be a breach of this policy (and therefore will be treated as a serious conduct issue). Since family relationships can be easily identified and recognised, adults must notify the Headteacher of any family relationship with a pupil so that the position can be formally acknowledged, discussed and recorded.

4.5.13. Staff should be very careful not to put other staff at risk by adding personal details of their colleagues to a social networking/online site.

4.5.14. Staff must be cautious about following or being followed by parents/carers of pupils, accepting parents of pupils as friends on Facebook or having contact with parents/carers on any social networking site.

4.5.15. Staff must be mindful at all times of the boundaries between their work and personal life in accordance with this policy.

4.5.16. Staff must also be cautious when inviting work colleagues to be friends on social networking sites. Social networking sites can blur the boundaries between work and personal lives and it may be difficult to maintain professional relationships.

4.5.17. Communication with parents, carers and external organisations should be subject to the same checks as would letters written on school-headed paper.

4.5.18. The school may undertake monitoring of emails/ICT use of Users to ensure a safe and secure system and to prevent misuse.

4.6. <u>Digital Images:</u>

4.6.1. Photographs or video footage of young people in schools can count as personal data under the Data Protection Act 1998. Therefore Users should refer to the Data Protection Policy (D001) which details how images should be used appropriately.

4.6.2. Users should not use images of students on websites, resource materials etc. without first ensuring that appropriate consent has been attained from students and parents. There must not be any images used of children in care or adopted.

4.6.3. Users may use school photographic or video technology to capture or support school trips and appropriate curriculum activities.

4.6.4. Users must not use personal digital equipment to record such images or videos unless express permission has been received from the Headteacher. Only school based equipment should be used and must be securely stored after use. Images taken on school equipment must be uploaded onto the school system at the earliest possible opportunity. Images must then be immediately deleted from the equipment

4.6.5. Users must not store images / videos of students on personal ICT devices at home or school. They should be stored centrally with the school's Community and Marketing Officer on the school network and deleted from other devices.

4.6.6. Images /videos of students MUST not be stored on pen drives or portable hard drives.

4.6.7. If Users require images at home to prepare materials and resources then specific permission should be obtained from the Headteacher before use and care must be taken to appropriately delete such images from ICT devices used outside of the school's network.

4.6.8. If photos or videos are needed for examination purposes, school digital technology must be used and photos and videos must be stored securely in school with agreement from the SLT Line Manager or the SLT member responsible for Digital Learning and Safety.

4.7. Users found to be in breach of this policy may be disciplined in accordance with the school's disciplinary procedure. In certain circumstances, breach of this policy may be considered gross misconduct resulting in termination of employment. Users must report all suspected breaches of this policy to the Headteacher.

5. Acceptable Use of Digital Technology for Students:

5.1. Allowing students' freedom to access digital resources brings the responsibility of using them safely and securely. Students are responsible for their own behaviour and conduct when using digital resources in the same way they are responsible for their own behaviour around school. We expect all students to adhere to the basic rules in this document.

5.2. An Acceptable Use Policy is about ensuring that you, as a student at Newall Green High School, can use the internet, email and other technologies available at the school in a safe and secure way. The policy also extends to out of school facilities e.g. our VLE, Internet, email, websites and mobile phones.

5.3. As a student at Newall Green High School, I agree that I will:

- Use all digital equipment and resources responsibly and safely.
- Report damage to equipment or the network immediately to a member of staff.
- Use only my own username and login to access the school network. I will be responsible for this username and password and not give it to anybody else.
- Only visit resources or websites which are appropriate to my work at the time as directed by my teacher.
- Report any misuse of the resources, including the internet, immediately to a member of staff.
- Only copy pictures or text into my area on the network. I will not download any other type of file. For example, software, games, screen savers etc.
- Ask a teacher before I print out any information from my area or the internet.
- Follow the Code of Conduct in ICT when learning in all ICT lessons – which focus on respect for each other and the equipment.
- Follow the health and safety guidelines for working with computers displayed in ICT rooms.

- Communicate safely through the VLE for school related issues only.
- Respect other people's views and beliefs
- Only post comments or messages which are appropriate to that discussion in online forum or discussion groups.
- Use E-mail for school use only. No inappropriate content should be included in any email.
- Be polite – never send, comment on or encourage others to send abusive messages.
- Report any breach (deliberate or accidental) of this policy to a teacher immediately.
- Report if I am sent inappropriate material e.g. images, videos etc. immediately to a member of staff within the school.
- When using my own personal devices in school must log on using the school bring your own device Wi-Fi network.

5.4. <u>As a student at Newall Green High School, I agree that I will NOT:</u>

- Attempt to log on using another person's username and password or access another person's files.
- Attempt to gain access to any part of the school network that is not available through my personal logon.
- Attempt to use or load programmes, files, tools or shortcuts to gain access to the internet or any other part of the network.
- Visit websites or resources that contain unsuitable material. If I am unsure if a site is suitable, I will ask a member of staff.
- Take information from the internet and pass it off as my own work. Plagiarised work is unacceptable.
- Retrieve, send, copy, display or post anything abusive, obscene, offensive or otherwise illegal.
- Post any personal or private information on myself or any other individual.
- Copy or forward messages without permission.
- Use or include any material which is confidential or copyrighted unless I have first obtained permission.
- Post any advertising or promotional material.
- Behave in an impolite or offensive manner.
- Take photographs, videos or other images/recordings of staff or students at school without permission.
- Post or download material which contains viruses or other programs which may disrupt the school's systems.
- Use the school system's in such a way that disrupts the use of the systems by other users.
- Use digital technology (including my mobile phone) in a manner that is likely to bring the school into disrepute or risk the welfare of another young person or myself.
- Use my mobile phone (or other mobile technologies) within school except at permitted breaks during the school day or when authorised by a member of staff as part of the learning.
- Download software or other files without permission
- Communicate to others any information which may result in the loss or damage to anyone else's work.
- Change the settings or preferences on any digital devices provided by the school. If this situation does occur a sanction will be put in place, parents will be brought in for a meeting and a ban may be put in place.

5.5. Mobile Technologies:

- The development of mobile technology is such that mobile phones and other similar devices can often include access to the internet, picture messaging, downloading of material and allow unregulated communication with others. The same guidance about use of the school's resources therefore applies to student's personal equipment within school.
- Any breach of these conditions will lead to students having their equipment confiscated by a senior member of staff.
- This policy may be updated or modified at any time should the school deem it necessary.
- The school reserves the right to administer these rules in a fair and unbiased way, which may result in a student's access to digital resources being removed or other appropriate sanctions being taken.
- Mobile phones/devices will not be used during lessons or formal times in school. The sending of abusive or inappropriate messages or files by text, Bluetooth, instant messaging, email or any other means is forbidden and will be dealt with in accordance with the school's Anti-Bullying and Behaviour Policies.
- Student use of cameras in their mobile phones must be strictly in line with this policy and will be kept under review.
- The school may undertake monitoring of emails belonging to all users of the system to ensure a safe and secure system and to prevent misuse

5.6. Declaration:

5.6.1. Parents/carers will be asked to sign and return the school's declaration form (Appendix E) stating that they have read and understood the school's 'Acceptable Use of Digital Technology For Students' document and the 'Parent /Carers Digital User policy' **and** give permission for their child to access ICT resources.

5.6.2. Any student who fails to abide by the school's Acceptable Use policy will have their access rights withdrawn and will be dealt with in line with the school's behaviour policy. Access rights will only be reinstated after appropriate discussion with parents/carers.

5.6.3. Staff will be required to sign and return the schools declaration form (Appendix D).

6. Digital Technology across the Curriculum:

6.1. Digital Technology has the potential to enhance the quality of teaching and learning across the curriculum. In addition, the ability to use technology effectively is becoming an assumed skill both in the work place and for lifelong learning. This must be reflected in the planning, delivery and assessment of any digital learning.

6.2. As a school we will provide our students with the basic skills and techniques needed to become effective users of a range of appropriate hardware/software. In addition, we provide opportunities to use ICT, within the wider curriculum of the school, so that students may develop the higher order skills necessary to engage successfully in digital media development, product development and programming.

6.3. In developing the ICT / digital technology skills of our students we aim to:

- Develop learners who are confident and discerning in their use of ICT
- Enable students to embrace ICT and become autonomous users

- Support a range of learning strategies including distance learning
- Give access to local, national and global information networks
- Enable access to resources to support lifelong learning
- Encourage problem-solving and investigation
- Enable communication and collaborative research with fellow students
- Foster sharing and collaboration between peers
- Foster caring and respect for equipment and resources
- Teach students to use the wealth of digital resources safely and securely

6.4. To embrace the school's commitment to Cross Curricular ICT it is important that the use of digital technology is embedded across all subject areas.

6.5. To enable this to happen all subject areas will:

- Embrace the use of digital technology in the pursuit of outstanding learning
- Experiment with new technologies within their own subject area
- Develop learners as independent enquirers using technologies to support their own learning
- Develop the key skills of ICT in their learning programmes
- Develop the Virtual Learning Environment as a key learning resource.
- Give students the skills and opportunities to be truly creative with ICT within different subject matter. Increasingly, we want students to be 'in the driving seat' in terms of finding new ways to advance their learning through ICT.

6.6. We recognise the importance of making our valuable, educational ICT facilities available to the students of Newall Green High School for learning out of school hours. Although many of our students have access at home to both a computer and Internet access, it is important that those who don't have the option of using the school's resources to further their learning.

6.7. The ICT facilities are available to the students out of school hours in both formal and informal ways. Many departments offer after school coursework catch-up and revision sessions, which will often involve the use of our ICT resources.

Parent/Carers Support

6.8. Parents/carers will be informed of the school's Digital Learning and Safety Policy which may be accessed on the school website.

6.9. Parents/carers will receive / have access to a copy of the 'Acceptable use of Digital Technology for Students' document (Appendix B) and the Parent/ carer Digital User Policy (Appendix C). Parents andstudents will be asked to sign the schools declaration forms (Appendix E)

6.10. Any issues concerning the misuse of ICT will be handled sensitively to inform parents/carers without undue alarm.

6.11. Advice on filtering systems and appropriate educational and leisure activities including responsible use of the Internet will be made available to parents/carers.

6.12. Interested parents/carers will be referred to organisations such as Child Exploitation and Online Protection (CEOP).

6.13. A partnership approach will be encouraged with parents/carers and this may include practical sessions as well as suggestions for safe internet use at home.

6.14. We will send out current advice to parents as necessary regarding social networking. Information will be obtained from a range of sources.

7. School ICT systems and resources:

7.1. As a school we manage a significant investment in the use of ICT. In many areas of work the use of ICT is vital and must be protected from any form of disruption or loss of service. It is therefore essential that the availability, integrity and confidentiality of the ICT systems and data are maintained at a level that is appropriate for our needs.

7.2. This requires highly effective development planning and resource investment as well as effective practices and routines for regular maintenance, swift and robust repair, safe and secure use and operation of the system.

7.3. The school resources available include:

- Whole School Networks
- Computers
- Printers
- Scanners
- Digital & Digital Video Cameras
- Music Technology
- CD/DVD Players
- Interactive Whiteboards
- Digital Projectors
- A wide range of software
- School Website
- Data Management Systems
- Externally hosted curriculum provision
- School Telephones

7.4. Effective and Efficient Deployment of ICT Resources:

7.4.1. ICT access is ensured through the schools hard-wired and Wi-Fi networks.

7.4.2. There is 1 dedicated ICT suite, and smaller Digital Learning areas in specific subject areas. The school endeavours to keep student access to computers to the ratio of 1 to 3 students.

7.4.3. The majority of hardware is purchased as part of a planned rolling programme of replacement. To this end, an annual review of needs will be made so that a systematic updating of equipment is implemented or decisions are made on group replacement.

7.4.4. The school has an alarm system and CCTV installed throughout. Each computer system has individual security to protect against access to the network system.

7.4.5. Staff wishing to use ICT resources can do so by booking the required facility via the booking system. Students cannot work unsupervised in any ICT room at any time and can only use ICT facilities within the school day to support curriculum studies in a clearly defined manner.

7.4.6. Printing of work should be kept to a minimum as this is draining on budgets. Where printing is required only completed final documents should be printed unless the syllabus or scheme of work require further hard copies to be produced.

7.5. Health and Safety:

7.5.1. All equipment will be checked appropriately under the Electricity at Work Regulation 1989 via the school's PAT testing schedule.

7.5.2. The Health and Safety at Work Act (1 January 1993), European Directive deals with requirements for computer positioning and quality of screen.

7.5.3. This directive is followed for all administration staff. Whilst this legislation only applies to people at work we seek to provide conditions for all children which meet these requirements

7.6. Disposal of equipment:

7.6.1. Prior to the transfer or disposal of any ICT equipment the School ICT Technicians will ensure that any personal data or software is obliterated from the machine if the recipient organisation is not authorised to receive the data.

7.6.2. Where the recipient organisation is authorised to receive the data for the purposes of data destruction, they must be made aware of the existence of any personal data to enable the requirements of the Data Protection Act to be met.

7.6.3. Normal write-off rules as stated in Financial Regulations apply and the item should be recorded appropriately on the Asset register.

7.6.4. Any Electrical equipment (including all ICT equipment) must be disposed of with regard to the Waste Electronic and Electrical Equipment (WEEE) regulations. All electrical equipment should therefore be referred to the ICT Technicians or the School's Estates Team to ensure correct disposal.

7.7. Administrative use of ICT:

7.7.1. The school uses a range of ICT to support the administrative functions of the school. The main resource the school uses is the CAPITA (SIMS) Management Information System, which is essentially a complex database of staff and student information. The School Data Manager (SIMS) is responsible for the safe and secure management and operation of the SIMS system and associated complementary packages, ensuring data integrity, acceptable & appropriate use, security and that the system is managed in line with Data Protection legislation. Access rights to SIMS are controlled by the School's Data Manager (SIMS) and are reviewed annually in conjunction with the ICT Infrastructure Leader.

7.7.2. The school uses a range of partner agencies such as the Local Authority and CAPITA SIMS to support and maintain its Data Management Infrastructure. Other MIS Systems are used throughout the school on a smaller scale.

7.7.3. The Data Manager (Assessment) is responsible for the safe and secure management of SISRA and other packages used to manage assessment data.

7.7.4. The School's Learning Resource Manager is responsible for the safe and secure operation of the School's library resource management system.

7.7.5. The ICT Technicians are responsible for the safe and secure operation of ALL other MIS systems relating to school provision e.g. Cashless Catering, email management systems, network user management systems.

8. Home Learning Safety:

8.1.1. All NGHS home learning resources are internet based and provided by external companies (E.g. Hegarty Maths, Microsoft Teams) and no private contact details of students are shared/used in the production of student profiles.

8.1.2. Home learning resources have the option to communicate with a teacher, but these communications are only possible within the software and are limited to text questions and in a set format (e.g. ask you teacher a question). These communications and responses from staff are recorded by the software and are saved.

8.1.3. NGHS as part of the PROSPERE Learning Trust uses Microsoft Teams, staff and students will use Microsoft Teams in accordance with the Standard Operating Procedure. This software is managed centrally within the Trust.

9. E-safety Responsibilities:

9.1. <u>E safety Responsibilities:</u>

9.1.1. The purpose of the use of ICT systems/digital technology in school is to help raise educational standards, promote student achievement, support the professional work of staff as well as enhance the school's management information and business administration systems.

9.1.2. All Users have a responsibility to maximise the educational and social benefit that can be obtained by exploiting the benefits and opportunities of using ICT, whilst minimising any associated risks to young people.

9.1.3. All members of the school community have a duty to be aware of e-safety at all times, to know the required procedures and to act on them. E-safety is a partnership concern and is not limited to school premises, school equipment or the school day.

9.1.4. Bullying, harassment or abuse of any kind via digital technologies or mobile phones will not be tolerated and complaints of cyber bullying will be dealt with in accordance with the school's Anti- Bullying and Behaviour Policies.

9.1.5. Complaints related to child protection will be dealt with in accordance with the school's Safeguarding Policy.

9.1.6. Students will be advised by staff to report Digital Safety issues to a member of staff or the SLT member responsible for Digital Learning & Safety.

9.1.7. Digital Safety is addressed in a variety of ways from assemblies, lessons in ICT or Academic Review and special drop-down days/sessions and advice to parents/carers.

9.1.8. Any misuse of the school's ICT systems must be reported immediately to the SLT member responsible for Digital Learning & Safety.

9.2. <u>Managing Internet Access:</u>

9.2.1. The internet offers a wide range of exciting teaching and learning opportunities, and

significant educational benefits from curriculum Internet use, including access to information from around the world and the ability to communicate widely. By providing internet and email access for staff and students, we are signalling our intention to provide the best learning resources possible. Internet safety depends on all staff, governors, users and parents to take responsibility for the safe use of the Internet.

9.2.2. Access to the internet supports educational and cultural exchanges between students world-wide and enables students to participate in cultural, vocational, social and leisure use in libraries, clubs and at home. It also offers opportunities for mentoring students and providing peer support for them and their teachers.

9.2.3. Internet use will be planned to enrich and extend learning activities and access levels will be reviewed to reflect the curriculum requirements and age of the children and young people.

9.2.4. The internet also supports professional development for staff through access to national developments, educational materials, good curriculum practice and exchange of curriculum and administration data with appropriate partner organisations. It can also improve access to technical support, including remote management of networks, supports communication with support services, professional associations and colleagues as well as allowing access to, and inclusion in, a range of government initiatives.

9.2.5. Internet safety is promoted in ICT lessons and form time. In addition, teachers should routinely raise issues surrounding use of the internet, including safety, with students when using ICT within the curriculum.

9.2.6. Developing good practice in internet use is essential for all students. Staff will guide students in on-line activities that will support the learning outcomes planned for the student's age and maturity. The school internet access is designed expressly for student use and includes filtering appropriate to the age of the children and young people.

9.2.7. Children and young people will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation. Students will be taught to be critically aware of the materials they read, how to validate information before accepting its validity as well as acknowledging the source of information used.

9.2.8. Students will be taught what to do if they experience material that they find distasteful, uncomfortable or threatening.

9.2.9. Students will be taught to consider the thoughts and feelings of others when publishing material to websites and elsewhere. Material which victimises or bullies someone, or is otherwise offensive, is unacceptable and appropriate sanctions will be implemented.

9.2.10. The internet connection at Newall Green High School is a 100MB leased line provided by BT 21cn. The school has a Smoothwall appliance installed locally, which acts as a web filter for all internet users in school as well as a firewall for edge security. E-mail is also hosted on-premises using Microsoft Exchange, and all incoming and outgoing mail is filtered through Microsoft Online Protection For Exchange.

9.2.11. Staff can also control internet access, select certain websites and view what is on each screen in the classroom using specialist networked software called LANSCHOOL.

9.2.12. The way that technology is deployed within the school is also to be considered. For example, allowing internet access for students only on those computers on clear public display, or re-siting existing machines, can reduce potential problems. ICT classrooms have been designed with this in mind.

9.3. Managing Website Content:

9.3.1. The headteacher or a senior member of staff will have overall editorial responsibility for the school's website and ensure that all content is accurate and appropriate. Editorial guidance will ensure that the school's ethos is reflected in the website, information is accurate, well presented and personal security is not compromised. Care will be taken to ensure that all information is considered from a security viewpoint including the use of photographic material.

9.3.2. Use of photographs will be carefully selected so that images of students are appropriate. Photographs of students will not be used without the written consent of the student's parents/carers.

9.3.3. The website will comply with the school's guidelines for publications and parents/carers will be informed of the school policy on image taking and publishing.

9.3.4. The point of contact on the school website will be the school address, school e-mail and telephone number. Staff or student's home information will not be published

9.3.5. The copyright of all material must be held by the school or be attributed to the owner where permission to reproduce has been obtained.

9.4. Social Networking and Communication Forums:

9.4.1. Social networking sites can present some risks if not used in a safe and responsible way. As with most new technologies, key issues centre around content and contact risks. One of the key benefits of social networking sites are that they encourage young people to be creative users of the internet, publishing content rather than being passive consumers. They can express themselves with an online personality, use all the applications the site has to offer, chat and socialise with peers, and share multimedia content such as music, photos and video clips with others.

9.4.2. However, there are concerns that young people may upload content to their online spaces that is inappropriate, offensive or even illegal, posting material that could damage their reputations or the reputations of others. Equally they may post inappropriate comments to the profiles of others, which can result in the bullying, slander or humiliation of others.

9.4.3. Another key area of concern is the permanency of content posted online – once published online a photo, a video clip or other content can be freely copied and circulated and will potentially exist forever.

9.4.4. Many young people maintain very detailed online profiles, including a large amount of personal information, photos and accounts of daily routines, which could lead to them being identified or contacted in person. The contact risks of other forms of new technology are well documented, and those that seek to harm or exploit children and young people will use social networking sites as another way to contact and groom potential victims.

9.4.5. Most social networking sites do contain privacy settings, allowing a profile to be set to private and only viewed by approved contacts, but these are not always used. Indeed, one of the big attractions of social networking sites is the large numbers of 'virtual' friends that can be linked from a profile, but this can expose children and young people to the risks of unwelcome contact.

9.4.6. A further risk includes the amount of time that children and young people may spend on social networking sites to the detriment of relationships with family, friends and peers in the real world.

9.5. Minimising risks to students at Newall Green High School:

9.5.1. In school time social networking sites should not be accessed other than as part of specific curriculum delivery. At Newall Green High School Social Network sites are blocked so that students cannot use them unsupervised. Such sites, newsgroups and educational networking sites are still used in lessons where students can be properly supervised and can be taught how to use such sites safely.

9.5.2. It is likely that children and young people will access social networking sites from other locations. As such, we have a duty to educate them as to the safe and responsible behaviours to adopt when using social networking services and other forms of new technologies as part of their ICT education, AR Curriculum and through Digital Safety Events.

9.5.3. Students are encouraged to talk about their online activity and staff are encouraged to educate them to the possible downsides - encouraging safe use and recognising the benefits, while being aware of the impact of their actions online and the possible risks and dangers. Using social networking sites responsibly forms part of our Digital Safety Curriculum at Newall Green High.

9.5.4. Safe Social Networking messages / discussions may include:

- Establishing with young people the sites they can sign up to
- Establishing the minimum ages that sites will accept and abiding by these restrictions
- Discussing the importance of privacy online and encouraging young people to make use of privacy settings
- Discussing the importance of personal safety when using social networking sites and chatrooms
- Teaching the principle that it is safer to only allow access to friends known in the 'real world'
- Regularly reviewing young people's online profiles along with them
- Encouraging young people to seek help if they experience any problems online
- Advising students to use nick names and avatars when using social networking sites

9.5.5. If curriculum areas have or want to set up an educational school social network account they should liaise with the SLT member responsible for Digital Learning and Safety. Staff must not communicate one on one with students and at least two staff members should have admin rights to the account. Any content used on the site must be reviewed, be age appropriate and checked that it does not contain links to inappropriate or unmonitored sites. Any misuse of the account must be reported immediately to the SLT member responsible for Digital Learning & Safety.

9.6. Photographic, Video and Audio Technology:

9.6.1. Images can be an excellent teaching tool. Effective use of images can make it easier to teach difficult concepts, can provide a stimulus for class discussion, or add visual appeal to a teacher's presentation or the individual work of students. The internet can provide a wonderful source of images, many of them copyright free, but finding appropriate images can be a challenge.

9.6.2. Many major search engines offer pre-set image searching from the homepage, often with safe searching options to filter results. However such searches and filters generally work on the basis of filename and description, and so can lead to misleading, unexpected or inappropriate results, sometimes of an adult nature. While you may find search engine image searches useful in lesson preparation, they should always be used with care and caution, and

they should NOT be used 'live' within a classroom setting.

9.6.3. An alternative to search engines is to use specialist web-based image collections – sites which deal specifically with key subjects such as the arts, animals, history or scientific concepts. These have the benefit of being closed collections, monitored and moderated by specialists within their field. Many now have an educational focus and provide copyright permissions specifically for educational use.

9.6.4. Videoconferencing and webcam use will be appropriately supervised for the student's age. When not in use all video conferencing cameras will be switched off. Students must have permission from a member of staff before making or answering a videoconference call or making a video or audio recording in school or on educational activities.

9.7. It is not appropriate to use photographic or video technology in changing rooms or toilets.

9.8. Film, TV or Internet sourced media:

9.8.1. The viewing of any Film, TV or Internet sourced video or media clips in the classroom must be clearly linked to the programme of study and appropriate to the lesson objectives. All media content should be viewed by staff prior to the lesson to ensure that it is appropriate to be shown to the group of students.

9.8.2. Where appropriate with films or broadcast TV age appropriate guidance must be followed. In terms of films this refers to the British Board of Film Certification (BBFC) classification. Staff must use caution and check materials before use.

9.8.3. In terms of PG films the BBFC advise that a 'PG' film should not disturb a child aged around eight or older. However, adults are advised to consider whether the content may upset more sensitive children. It is therefore highly advisable to consider the nature of your group and how the content may affect the students in it before viewing it in the lesson.

9.8.4. Some internet sources of 'clips' or 'snippets' may not be clear about guidance ratings. It is the responsibility of the member of staff showing such clips to ensure it is age appropriate. In particular You Tube clips from independent sources will have no guidance or certification and MUST be viewed by staff before being shown to students. Staff should only show such content to students if they are happy that it is age appropriate. If staff have any doubts then they should refer to a member of SLT for guidance.

9.8.5. If staff members have any concerns about the above guidance or have reason to show a clip that does not fall into the age appropriate guidance, they must discuss this with a member of SLT and consideration would be given to gaining parental consent to support this.

9.9. Assessing Risks:

9.9.1. Emerging technologies offer the potential to develop teaching and learning tools but need to be evaluated to assess risks, establish the benefits and to develop good practice. All Users should be aware that technologies such as mobile phones with wireless internet access can bypass school filtering systems and allow a new route to undesirable material and communications. Therefore we have to be vigilant about student use of new technologies and ensure that school use of such technologies are implemented safely and securely.

9.9.2. In common with other media such as magazines, books and video, some material available through the Internet is unsuitable for students. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to international scale and linked nature of Internet content, it is not always possible to guarantee that unsuitable material may never appear on a school computer. The school cannot accept liability for

Internet material accessed, or any consequences of Internet access.

9.9.3. Emerging technologies will be examined for educational use and a risk assessment will be carried out before use in school is allowed and methods to identify, assess and minimise risks will be reviewed regularly.

9.9.4. A risk assessment will be carried out before children and young people are allowed to use new technology in schools and settings.

9.10. Dealing with Complaints:

9.10.1. Concerns related to ICT systems or misuse of ICT should be directed to the SLT member responsible for Digital Learning and Safety. General complaints will be dealt with in line with the school's complaints policy. Safeguarding concerns must be dealt with through the school's Safeguarding Procedures.

9.10.2. The SLT member responsible for Digital Learning and Safety will be responsible for dealing with most complaints and any complaint concerning staff or student misuse of ICT will be reported to the Headteacher immediately.

9.10.3. As with other serious issues, there may be occasions when the school must contact the police. If appropriate, early contact should be made to discuss strategies and preserve possible evidence.

9.10.4. Sanctions for misuse may include any or all of the following:

- Interview/counselling by an appropriate member of staff / agency
- Informing parents/carers
- Removal of internet/computer access for a specified period of time, which may ultimately prevent access to files, held on the system, including examination coursework.
- Disciplinary processes
- Referral to the police
- Referral to Safeguarding Agencies such as Children's Services

9.11. The Prevent Duty:

9.11.1. Schools have a vital role to play in equipping children and young people to stay safe online, both in and outside school and also in protecting pupils from the risks of extremism and radicalisation. Section 26 of the Counter-Terrorism and Security Act 2015 places a duty on specified authorities, (including schools) in the exercise of their functions, to have due regard to the need to prevent people from being drawn into terrorism (the Prevent Duty).

9.11.2. Terrorist organisations, such as ISIL, are attempting to radicalise and recruit young people through extensive use of social media and the internet. As with any other online risks of harm, every adult in school (teachers and teaching assistants in particular) must be aware of the risks posed by the online activity of extremist and terrorist groups.

9.11.3. The Government has issued statutory guidance in relation to the Prevent Duty (June 2015). In addition, to assist schools and to help recipients understand the implications of the duty, the DfE has also produced non statutory advice (June 2015).

9.11.4. The statutory guidance makes clear the need for schools to ensure that children are safe from terrorist and extremist material when accessing the internet in schools. The school will

ensure that suitable filtering is in place. Internet safety is integral to the school's ICT curriculum and the school will ensure it is embedded in the school curriculum. *In addition to advice on internet safety provided by the school, further general advice and resources for schools on internet safety are available on the UK Safer Internet Centre website*

9.11.5. Keeping children safe from risks posed by terrorist exploitation of social media should be approached by adults in school in the same way as safeguarding children from any other form of online abuse. The DfE has produced a briefing note aimed mainly at Headteachers, teachers and safeguarding leads in schools detailing how social media platforms are being used in particular to encourage travel to Syria and Iraq. All adults in school (teachers and teaching assistants in particular), should familiarise themselves with the contents of the briefing note and must ensure that if they have any concerns, the school's normal safeguarding procedures are followed. *The Briefing Note is available on the school website.*

9.11.6. For the avoidance of doubt, if any adult working in school has a concern that a particular pupil or group of pupils is at risk of radicalisation or terrorist exploitation, through social media or otherwise, they must immediately contact the Headteacher and follow the school's normal safeguarding procedures, including discussing the matter with the school's designated safeguarding lead and where deemed necessary, with children's social care at the Local Authority and the local police.

10. Monitoring and Review:

10.1. This policy will be held under operational review by the SLT member responsible for Digital Learning and Safety. The policy will be reviewed in line with the Governing Body Workplan.

Appendix A: Resources

Listed below are a selection of organisations/resources that provide useful information relating to ICT use within school.

Association of Co-ordinators and Teachers of IT (ACITT) http://www.dbprimary.com/
Wide range of information on educational and administrative ICT issues

BECTA (Now all archived) www.becta.org.uk
Advice and guidance on computer misuse

British Computer Society http://www.bcs.org/
Advice and guidance for headteachers, governors, and ICT co-ordinators on writing school ICT acceptable use policies.

Childnet http://www.childnet.com/
Advice to children, parents and teachers about the safe use of the internet.

The Computer Emergency Response Team http://www.cert.org/
US site providing in depth, up-to-date information on protecting against viruses

Computer Misuse Act 1990 http://www.legislation.gov.uk/ukpga/1990/18/contents
The full text of the Act

Information Commissioner on the Data Protection Act http://ico.org.uk/for_organisations/data_protection
Employment Practices Data Protection Code – Part 3: Monitoring at Work

Intellectual Property Office http://www.ipo.gov.uk/ipenforce-group.htm
A Government site providing specific information about intellectual property on the internet

Internet Watch Foundation https://www.iwf.org.uk/
Information on illegal material on the internet. This site also invites people to report inappropriate web sites. Funded by DTI

Kent County Council
http://www.kent.gov.uk/education-and-children/protecting-children/online-safety
Comprehensive information on implementing an internet Access Policy

National Association of Advisers for Computers in Education (NAACE) http://www.naace.co.uk/
Guidelines on using the internet safely and insurance issues

National Grid For Learning (Now all archived)
https://www.education.gov.uk/consultations/downloadableDocs/42_1.pdf
Advice on all aspects of Internet safety for schools and LEAs.

Northamptonshire County Council
http://www.northamptonshire.gov.uk/en/councilservices/social- care/plans/policy/Pages/PolicyLibrary.aspx
A basic toolkit for headteachers, staff and governors, to help them comply with data protection requirements and related legislation.

360 degrees safe http://www.360safe.org.uk/
An e-safety self-review tool for schools

Appendix B- Acceptable Use of Digital Technology for Students

Allowing students' freedom to access digital resources brings the responsibility of using them safely and securely. Students are responsible for their own behaviour and conduct when using digital resources in the same way they are responsible for their own behaviour around school. We expect all students to adhere to the basic rules in this document.

An Acceptable Use Policy is about ensuring that you, as a student at Newall Green High School, can use the internet, email and other technologies available at the school in a safe and secure way. The policy also extends to out of school facilities e.g. our VLE, Internet, email, websites and mobile phones.

As a student at Newall Green High School, I agree that I will:

- Use all digital equipment and resources responsibly and safely.
- Report damage to equipment or the network immediately to a member of staff.
- Use only my own username and login to access the school network. I will be responsible for this username and password and not give it to anybody else.
- Only visit resources or websites which are appropriate to my work at the time as directed by my teacher.
- Report any misuse of the resources, including the internet, immediately to a member of staff.
- Only copy pictures or text into my area on the network. I will not download any other type of file. For example software, games, screen savers etc.
- Ask a teacher before I print out any information from my area or the internet.
- Follow the Code of Conduct in ICT when learning in all ICT lessons – which focus on respect for each other and the equipment.
- Follow the health and safety guidelines for working with computers displayed in ICT rooms.
- Communicate safely through the VLE for school related issues only.
- Respect other people's views and beliefs
- Only post comments or messages which are appropriate to that discussion in online forum or discussion groups.
- Use E-mail for school use only. No inappropriate content should be included in any email.
- Be polite – never send, comment on or encourage others to send abusive messages.
- Report any breach (deliberate or accidental) of this policy to a teacher immediately.
- Report if I am sent inappropriate material e.g. images, videos etc. immediately to a member of staff within the school.
- When using my own personal devices in school must log on using the school bring your own device Wi-Fi network.

As a student at Newall Green High School, I agree that I will NOT:

- Attempt to log on using another person's username and password or access another person's files.
- Attempt to gain access to any part of the school network that is not available through my personal logon.
- Attempt to use or load programmes, files, tools or shortcuts to gain access to the internet or any other part of the network.
- Visit websites or resources that contain unsuitable material. If I am unsure if a site is suitable, I will ask a member of staff.
- Take information from the internet and pass it off as my own work. Plagiarised work is unacceptable.
- Retrieve, send, copy, display or post anything abusive, obscene, offensive or otherwise illegal.
- Post any personal or private information on myself or any other individual.
- Copy or forward messages without permission.
- Use or include any material which is confidential or copyrighted unless I have first obtained permission.
- Post any advertising or promotional material.
- Behave in an impolite or offensive manner.
- Take photographs, videos or other images/recordings of staff or students at school without permission.
- Post or download material which contains viruses or other programs which may disrupt the school's systems.

- Use the school system's in such a way that disrupts the use of the systems by other users.
- Use digital technology (including my mobile phone) in a manner that is likely to bring the school into disrepute or risk the welfare of another young person or myself.
- Use my mobile phone (or other mobile technologies) within school except at permitted breaks during the school day or when authorised by a member of staff as part of the learning.
- Download software or other files without permission.
- Communicate to others any information which may result in the loss or damage to anyone else's work.
- Change the settings or preferences on any digital devices provided by the school. If this situation does occur a sanction will be put in place, parents will be brought in for a meeting and a ban may be put in place.

Appendix C- Parent/ Carer Policy

The Purpose of the Policy

Social media and social networking sites play an important role in the lives of many people. We recognise that sites bring risks, but equally there are many benefits to be reaped. This policy gives clarity to the way in which social media/mobile phones are to be used by pupils, governors, visitors, parent helpers and school staff at Newall Green High School. It will also provide guidance for parents.

There are four key areas:

A. The use of social networking sites by pupils within school

B. Use of social networking by staff in a personal capacity

C. Comments posted by parents/carers

D. Dealing with incidents of online bullying

A. The use of social networking sites by pupils within school

The school's Digital Learning and Safety Policy and the Acceptable Use of Digital Technology for Students outlines the rules for using IT in school and these rules therefore apply to use of social networking sites. Both documents are available online.

In terms of private use of social networking sites by a child it is generally understood that children under the age of 13 are not permitted to be registered, including Facebook, Instagram and whatsapp to name a few examples. Students using personal devices in school outside of lesson times must log on using the schools Bring Your Own Device WI-FI network. Students must abide by the Acceptable Use of Digital Technologies document when using such sites.

B. Use of social networking by staff in a personal capacity

It is possible that a high proportion of staff will have their own social networking site accounts. It is important for them to protect their professional reputation by ensuring that they use their personal accounts in an appropriate manner.

Guidelines are issued to staff:

- Staff must **never** add pupils as ‘friends’ into their personal accounts (including past pupils under the age of 21).
- Staff are **strongly advised** not to add parents as ‘friends but where there is a strong link out of school then the head teacher must be advised of this.
- Staff **must not** post comments about the school, pupils, parents or colleagues including members of the Governing Body.
- Staff should only use social networking in a way that does not conflict with the current National Teacher's Standards.
- Staff should review and adjust their privacy settings to give them the appropriate level of privacy and confidentiality.
- Staff should read and comply with 'Guidance for Safer Working Practice for Adults who Work with Children and Young People'.
- Staff should keep the school and social media separate, including not identifying place of work on social media sites.

- If posting professionally school authorized accounts should be used.
- It is the responsibility of all staff members to report the any misuse of social networking they become aware of to the Headteacher.
- Inappropriate use by staff should be referred to the Headteacher in the first instance and may lead to disciplinary action.

C. Comments posted by parents/carers

Parents and carers will be made aware of their responsibilities regarding their use of social networking. Methods of school communication include the prospectus, the website, newsletters, letters and verbal discussion. School policies and documents provide further information regarding appropriate channels of communication and means of resolving differences of opinion. Effective communication following principles of mutual respect is the best means of ensuring the best learning experiences for the child.

Parents must not post pictures of pupils, other than their own children, on social networking sites where these photographs have been taken at a school event.

Parents must not name students by tagging or making comments on sites used by the school.

Parents should make complaints through official school channels rather than posting them on social networking sites.

Parents should not post malicious or fictitious comments on social networking sites about school or any member of the school community. School may take action against any parent making malicious or defamatory comments including reporting to the appropriate authorities and legal action.

D. Dealing with incidents of online bullying/inappropriate use of social networking sites

The school's Anti-Bullying Policy sets out the processes and sanctions regarding any type of bullying by a child on the school roll.

In the case of inappropriate use of social networking by parents, the Governing Body will contact the parent asking them to remove such comments and seek redress through the appropriate channels such as the Complaints Policy and will send a letter.

The Governing Body understands that, "There are circumstances in which police involvement is appropriate. These include where postings contravene the Prevent duty, have a racist element or where violence is threatened or encouraged." Furthermore, "Laws of defamation and privacy still apply to the web and it is unlawful for statements to be written which:

- attempt to radicalise and recruit young people through extensive use of social media and the internet.
- expose (*an individual*) to hatred, ridicule or contempt
- cause (*an individual*) to be shunned or avoided
- lower (*an individual's*) standing in the estimation of right-thinking members of society or
- Disparage (*an individual in their*) business, trade, office or profession." (National Association of Headteachers)

Appendix D

User Declaration- Staff

- I have read the school's current Digital Learning and Safety Policy (A007). I know that this policy is stored on the school's T drive for reference.
- I understand and agree to the conditions of this policy. I understand that any breach of these conditions may result in disciplinary action in accordance with the school's disciplinary procedure and the removal of my access to ICT facilities. I understand that in certain circumstances, breach of this policy may be considered gross misconduct resulting in termination of employment.
- I understand that it is the duty of all Users to ensure children and young people at Newall Green High School are safe and secure when using our ICT systems. I agree to report any misuse of the system or concerns about e-safety immediately to a senior staff member.

NAME: _____

SIGNATURE: _____

DATE: _____

Appendix E

Student Declaration

I have read the school's policies related to Digital learning and Safety specifically:

The Acceptable User Policy for Students

The Parent and Carer Policy

The full Digital Learning and safety Policy is available on the school website if I wish to access it.

Student Declaration

- I understand and agree to the conditions of the Acceptable User Policy for Students.

NAME: _____

SIGNATURE: _____

DATE: _____

Parent Declaration

Parent declaration

- I **do / do not** give permission for my son/ daughter to access ICT including internet at school. (please delete as appropriate)

- I understand and agree to the conditions of the Acceptable User Policy for Students and the Parent / Carer Digital user Policy

NAME: _____

SIGNATURE: _____

DATE: _____