HAWTHORNS
SCHOOL

Approved December 2019

Review date: September 2021

Signed Chair of Governors:

E-Safety Policy

Document Control Information

E- Safety Policy, Issue 3– December 2019

Review Period Two years	**Review Committee** MAT Trustees

Revision History

Author	Summary of changes	Issue	Date Authorised
R Bright	New policy	1	14th July 2015
R Bright	Policy framework audit	2	31 August 2017
R Righini	Policy review	3	19th Sep 2018
R Bright/ A Cooke	Policy review/incorporate Hawthorns	4	9th December 2019

Authorisation

Approved By:	*Governors*
Approved:	*December 2019*
Date of Next review:	*September 2021*
Document Owner & Reviewer:	*Hawthorns School*

Equality Impact

Statement

We welcome feedback on this document and the way it operates. We are interested to know of any possible or actual adverse impact that may affect any groups in respect of any of the Equality Act 2010 protected characteristics.

The person responsible for equality impact assessment for this document is the Director of Equality and Diversity.

Screening

This document has been screened by the Equality Team and the impact has been assessed as:

- ☐ Not applicable
- ☐ Low
- ☐ Medium
- ☐ High

1. Purpose

1.1. New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

1.2. The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps all staff and young people learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

1.3. The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. A school e-safety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education from the Executive Principal, Heads of Site and governors to the senior leaders and deliverers, support staff, parents/carers members of the community and the young people themselves.

1.4. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote achievement. However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

1.4.1. Access to illegal, harmful or inappropriate images or other content
1.4.2. Unauthorised access to / loss of / sharing of personal information
1.4.3. The risk of being subject to grooming by those with whom they make contact on the internet.
1.4.4. The sharing / distribution of personal images without an individual's consent or knowledge
1.4.5. Inappropriate communication / contact with others, including strangers
1.4.6. Sexting
1.4.7. Cyber-bullying
1.4.8. Access to unsuitable video / internet games
1.4.9. An inability to evaluate the quality, accuracy and relevance of information on the internet
1.4.10. Plagiarism and copyright infringement
1.4.11. Illegal downloading of music or video files
1.4.12. The potential for excessive use which may impact on the social and emotional development and learning of the young person.
1.4.13. The threat of radicalisation and extremism.

1.5. Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies (eg behaviour, anti-bullying and child protection).

1.6. As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build an understanding of the risks to which the young people may be exposed, so that they have the confidence and skills to face and deal with these risks.

1.7. The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The e-safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

2. Scope of Policy

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

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

2.3. The school will, where known, inform agencies, parents / carers of incidents of inappropriate e-safety behaviour that takes place out of school.

3. Reason for Review

3.1. This policy was reviewed as part of a policy framework audit.

4. Aim(s)

4.1. The aim of this policy is to ensure that staff and young people access ICT systems safely and within agreed constraints.

5. Procedures and practice

5.1. Roles and Responsibilities

5.1.1. Trustees - Trustees have overall responsibility for the approval of the E-Safety Policy. The Governing Body will receive regular information about e-safety incidents.

5.1.2. Head of Site - The Head of Site is responsible for ensuring the safety (including e-safety) of members of the school community and ensuring that appropriate procedures are in place for reporting e-safety incidents.

5.1.3. The Head of Site will ensure that key e-safety messages are reinforced as part of a planned programme of assemblies

5.1.4. The Head of Site will be trained in e-safety issues and be aware of the potential for serious child protection issues arising from;

5.1.4.1. Sharing of personal data.
5.1.4.2. Access to illegal / inappropriate materials.
5.1.4.3. Inappropriate on-line contact with adults / strangers.

5.1.4.4. Potential or actual incidents of grooming.
5.1.4.5. Cyber-bullying.

5.1.5. The Head of Site, with the support of the E-safety Co-ordinator, will deal with any investigations, actions or sanctions of reported incidents.

5.1.6. The E-Safety Co-ordinator and other supporting e-safety staff will ensure that they have relevant qualifications to train staff, young people and parents/carers.

5.1.7. The E-Safety Co-ordinator will sit on the technical board and have a leading role in establishing and reviewing the school e-safety policy. They will liaise closely with the local authority and the ICT technical team with regards to all aspects of e-safety.

5.1.8. The E-Safety Co-ordinator will ensure that;
5.1.8.1. all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
5.1.8.2. procedures are in place for signing acceptable use forms
5.1.8.3. training and advice is provided for staff
5.1.8.4. e-safety incidents are logged and creates a report of incidents to inform future e-safety developments
5.1.8.5. when serious incidents have been raised that these are reported to the Head of Site and/or the Senior Leadership Team

5.1.9. Network Manager / Technical staff: - The Network Manager is responsible for ensuring:
5.1.9.1. That the school's ICT infrastructure is secure and is not open to misuse or malicious attack
5.1.9.2. That the school meets the e-safety technical requirements outlined in the security and acceptable use sections of this policy.
5.1.9.3. That users only access the school's networks through enforced password protection.
5.1.9.4. That filtering is applied and updated on a regular basis in line with the section on filtering.
5.1.9.5. That they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.
5.1.9.6. That the use of the network / Virtual Learning Environment (VLE) / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Head of Site.
5.1.9.7. That monitoring software / systems are implemented and updated.
5.1.9.8. That servers, wireless systems and cabling are securely located and physical access restricted.

5.1.9.9. That they give all users clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the Network Manager and will be reviewed, at least annually, by the Technical group.

5.1.10. Teaching and Support Staff are responsible for ensuring that:

5.1.10.1. They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices.

5.1.10.2. They have read, understood and signed the Staff Acceptable Use Agreement (Appendix 1) as part of their Induction.

5.1.10.3. They report any suspected misuse or problem to the Head of Site.

5.1.10.4. Digital communications with the young people (Email / Virtual Learning Environment) should be on a professional level and only carried out using official school systems.

5.1.10.5. E-Safety issues are embedded in all aspects of the curriculum and other school activities.

5.1.10.6. Where applicable, young people understand and follow the school e-safety codes.

5.1.10.7. Where applicable, young people have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

5.1.10.8. They monitor ICT activity in lessons, extra-curricular and extended school activities.

5.1.10.9. They are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices.

5.1.10.10. In lessons where internet use is pre-planned young people should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

5.1.11. Technical Group - Members of the technical Group will assist the E-Safety Co-ordinator with:

5.1.11.1. Reviewing and monitoring the Total E-Safety Policy.

5.1.11.2. The planning and delivery of e-safety training across the organisation.

5.1.11.3. The reviewing and monitoring of the SHARP (School Help and Advice Reporting Page) and reported incidents.

5.1.11.4. There will be regular reviews and audits of the safety and security of school ICT systems.

5.1.12. Young People, where appropriate:

5.1.12.1. Are responsible for using the school ICT systems in accordance with the teacher’s instructions and e-safety codes of conduct.

5.1.12.2. Should have an understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

5.1.12.3. Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

5.1.12.4. Will be expected to know and understand the acceptable use of mobile phones, digital cameras and hand held devices including the use of images.

5.1.12.5. Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.

5.1.13. Parents / Carers - play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, and website/VLE and e-safety workshops. Parents and carers will be responsible for:

5.1.13.1. Endorsing the Hawthorns e-safety policy

5.1.13.2. Accessing the school website and e-safety resources

5.2. **Curriculum**

5.2.1. E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum:

5.2.1.1. in lessons where internet use is pre-planned, it is best practice that the young people should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

5.2.1.2. where young people are allowed to freely search the internet, eg using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.

5.2.1.3. it is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination, social networking). In such a situation, staff can request that the Network Manager can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

5.3. **Use of school Mobile Devices**

5.3.1. The New Bridge Group offers a 1:1 iPad for all young people and staff. The use of the iPad provides an opportunity to enhance the overall learning experience but it is important that the device is used responsibly and measures are taken to ensure the security of the device and any data stored on the iPad.

5.3.2. The device will be provided to you in a protective case and must remain inside the case at all times. Handle the iPad with care and respect. Do not throw, damage, place heavy items on, or intentionally drop your device.

5.3.3. It is important you keep your iPad safe at all times. You should know where your iPad is at all times and ensure the battery is charged, and ready for use each and every morning. Class teachers are responsible for ensuring the young people in their class have their iPad with them or stored in the lockers whenever it is not being used.

5.3.4. If a pupil or staff device becomes damaged, lost or stolen, report it to the Head of Site and the Technical Group as a matter of urgency. The iPad is insured by the school when the device is lost, damaged or stolen when on the school site or during educational visits. If the device is lost, damaged or stolen whilst at home, it is your responsibility to replace or repair the device from your personal home insurance. Staff should not keep or leave the iPad unattended in vehicles. If your device has become damaged, lost or stolen you must report it to the Technical Group immediately. You must not carry out repairs on any school-owned device. You must not solicit any individual or company to repair a school-owned device on your behalf.

5.3.5. All iPads will be enrolled into the schools ‘Mobile Device Management’ system. At no point should you attempt to remove your device from this system. All iPads are managed by the Technical Group. The school provides a managed Apple ID and 200GB of iCloud storage. You should ensure your files are backed up to your iCloud or to the secure New Bridge IT systems (staff drive/home drive). Do not link up personal third-party apps or services, such as Dropbox or any unauthorised personal cloud storage.

5.3.6. Your iPad passcode will be provided by the Technical Group and must not be changed without permission from the technicians.

5.3.7. The username and password for staff laptops and ipads is their New Bridge email and Nb number.

5.3.8. Usage of the iPad is subject to the conditions outlined in the school’s Total E-Safety Policy and Acceptable Use Agreements. Anyone in breach of this policy may be subject, but not limited to disciplinary action, confiscation, removal of content, or referral to the police or other external agencies.

5.3.9. Your iPad device is not for personal use and has been provided for work-related use only.

5.3.10. Do not give anyone else access to your iPad, unless expressly authorised to do so by the Head of Site. Staff are prohibited from taking or storing personal photos/videos on school devices.

5.3.11. Young people are restricted from accessing the App store and apps will only be distributed by self-service. Any free and paid apps to be put on the self service will need to be authorised by the ICT Co-ordinator on site.

5.4. **Use of digital and video images**

5.4.1. The development of digital imaging technologies has created significant benefits to learning, allowing staff and young people instant use of images that they have recorded themselves or downloaded from the internet. However, staff and young people need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

5.4.2. When using digital images, staff should inform and educate the young people about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.

5.4.3. Care should be taken when taking digital / video images that young people are not participating in activities that might embarrass the pupil or the school. Never record a young person in distress. Images taken are for recording achievement and progress.

5.4.4. Staff should never send images to parents. Images which are to be used on social media need to ensure they adhere to this policy.

5.4.5. Young people must not take, use, share, publish or distribute images of others without their permission or the permission of the teacher.

5.4.6. The young people's full names will not be used anywhere on a website or blog, particularly in association with photograph.

5.4.7. Written permission from parents or carers will be obtained before photographs of young people are published.

5.4.8. *All staff working with young people at Hawthorns must not take photos on their personal devices. Photographs of pupils are only to be taken on digital cameras or iPads provided by the school and must only be transferred to New Bridge IT systems.*

5.5. **Digital Communication**

5.5.1. Communication with young people, by whatever method, should take place within professional boundaries and staff should avoid any personal subject matter.

5.5.2. Staff should be mindful in their communications with young people so as to avoid any possible misinterpretation of their motives or any behaviour which could be construed as grooming.

5.5.3. Staff should not give their personal contact details to current pupils or past pupils including email, home or mobile telephone numbers unless the need to do so is agreed with senior management. Internal email systems should only be used in accordance with New Bridge Group policy.

5.5.4. Staff must only use their New Bridge Group or Hawthorns email account when communicating electronically with young people, parents and colleagues.

5.6. **Staff use of social media in the school**

5.6.1. Staff are permitted to access social media within school building but must be outside of lessons or other structured sessions. Excessive use of social media, which could be considered to interfere with productivity, will be considered a disciplinary matter.

5.6.2. Staff should assume that anything they write on social media (regardless of their privacy settings) could become public so should ensure that they are professional.

5.6.3. Any use of social media made in a professional capacity must not:

5.6.3.1. Bring the school into disrepute.
5.6.3.2. Breach confidentiality
5.6.3.3. Breach copyrights of any kind.
5.6.3.4. Bully, harass or be discriminatory in any way.

5.6.4. Staff should only use their class Twitter account for social media use to communicate class activities and learning. No other accounts should be associated with class or staff in a professional capacity.

5.7. **Staff use of social media outside of school**

5.7.1. The school appreciates that staff may make use of social media in a personal capacity. However, staff must be aware that if they are recognised from their profile as being associated with the school, opinions they express could be considered to reflect the school's opinions and so could damage the reputation of the school. For this reason, staff should avoid mentioning the school by name, or any member of staff by name or position. When using social media staff and others should:

5.7.1.1. Never share work log-in details or passwords.
5.7.1.2. Keep personal phone numbers private.
5.7.1.3. Never give personal email addresses to pupils or parents.
5.7.1.4. Restrict access to certain groups of people on their social media sites and pages.

5.7.2. Those working with children have a duty of care and are therefore expected to adopt high standards of behaviour to retain the confidence and respect of colleagues and pupils both within and outside of school. They should maintain appropriate boundaries and manage personal information effectively so that it cannot be misused by third parties for 'cyber-bullying', for example, or identity theft.

5.7.3. Staff should not make ‘friends’ of current pupils or past pupils at the school because this could potentially be construed as ‘grooming’, nor should they accept invitations to become a ‘friend’ of any pupils or parents.

5.7.4. Staff should also keep any communications with pupils and parents transparent and professional and should only use the school’s systems for communications. Communication should be limited to between the times of 8.30am and 5.00pm.

5.7.5. If there is any doubt about whether communication between a pupil/parent and member of staff is acceptable and appropriate the Head of Site should be informed so that they can decide how to deal with the situation.

5.7.6. Before joining the school, new employees should check any information they have posted on social media sites and remove any post that could cause embarrassment or offence.

5.8. **Use of Social Media – Young People**

5.8.1. No young person under 13 should be accessing social networking sites such as Facebook. There is a mechanism on Facebook where pupils can be reported via the help screen.

5.8.2. Where a disclosure of cyber-bullying is made, all schools now have the duty to investigate and protect, even where the cyber-bullying originates outside the school. Once a disclosure is made, the investigation will involve the families. This should be dealt with through the Group’s Anti-Bullying Strategy. If a parent/carer refuse to engage and bullying continues, it can be referred to the police as harassment

5.9. **Use of Social Media – Parents**

5.9.1. The Group recognises that many parents and other family members will have social networking accounts which they might use to discuss/share views about Group issues with friends and acquaintances. However, it is not the way to raise concerns or complaints as the Group will not respond to the issues raised on social networking sites. If there are any serious allegations being made/concerns being raised, social media or internet sites should not be used to name individuals and make abusive comments.

5.9.2. Although social networking sites may appear the quickest and easiest way to express frustrations or concerns about the Group and organisations associated with it, it is rarely appropriate to do so. Other channels, such as a private and confidential discussion with the teacher, Head of Site, a governor or by using the formal complaints process are much better suited to this.

5.9.3. We consider the following examples to be inappropriate uses of social networking sites. (This list is non-exhaustive and intended to provide examples only):

- *5.9.3.1.* Naming children or posting any comments about children who attend any organisation within the Group
- *5.9.3.2.* Making an allegation about staff or anyone else connected with the Group
- *5.9.3.3.* Making any post that could be deemed to be cyberbullying
- *5.9.3.4.* Making complaints about the Group; or the staff at the Group
- *5.9.3.5.* Making defamatory statements about the Group or the staff at the Group
- *5.9.3.6.* Posting negative or offensive comments about staff or any other individual connected to the Group
- *5.9.3.7.* Posting racist comments
- *5.9.3.8.* Posting comments which threaten violence

5.9.4. Parents should also ensure that their children are not using social networking sites in an inappropriate manner. It is expected that parents/carers explain to their children what is acceptable to post online. Parents/carers are also expected to monitor their children's online activity, including in relation to their use of social media.

5.9.5. The New Bridge Group will always try to deal with concerns raised by parents in a professional and appropriate manner and understands that parents may not always realise when they have used social networking sites inappropriately. Therefore, as a first step we will usually discuss the matter with the parent to try and resolve it and to ask that the relevant information be removed from the social networking site in question. If the parent refuses to do this and continues to use social networking sites in a manner that we consider inappropriate, we will consider taking the following action:

- *5.9.5.1.* Take legal advice and/or legal action where the information posted is defamatory in any way or if the circumstances warrant this
- *5.9.5.2.* Set out our concerns to the parent in writing, giving a warning and requesting that the material in question is removed
- *5.9.5.3.* Contact the police where the Group feels it appropriate - for example, if it considers a crime (such as harassment) has been committed or in cases where the posting has a racial element, is considered to be grossly obscene, grossly offensive or is threatening violence
- *5.9.5.4.* If the inappropriate comments have been made on a Group website or online forum, the Group may take action to block or restrict that individual's access to that website or forum
- *5.9.5.5.* Contact the host/provider of the social networking site to complain about the content of the site and ask for removal of the information.
- *5.9.5.6.* Take other legal action against the individual

5.10.**Data Protection**

5.10.1. Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018, which is the UK's implementation of the General Data Protection Regulation (GDPR). Everyone responsible for using personal data has to follow strict rules called 'data protection principles'. They must make sure the information is:

5.10.1.1. Used fairly, lawfully and transparently Processed for limited purposes

5.10.1.2. Used for specified, explicit purposes

5.10.1.3. Used in a way that is adequate, relevant and limited to only what is necessary Processed in accordance with the data subject's rights

5.10.1.4. Accurate and, where necessary, kept up to date

5.10.1.5. Kept for no longer than is necessary

5.10.1.6. Handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

5.10.2. Staff should refer to the school's data protection policy for further guidance

5.11.**School Filtering**

5.11.1. The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so. It is therefore important that school filtering manages the associated risks and to provide preventative measures which are relevant to the situation in this school.

5.11.2. The school receives the benefits of a managed filtering service, with flexibility for changes at local level.

5.11.3. The responsibility for the management of the school's filtering will be held by the Technical Committee.

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

5.11.4.1. Be logged in the Changed Control Log

5.11.4.2. Be reported to the Technical Committee.

5.11.4.3. Be reported to the Governors annually in the form of an audit of the changed control logs

5.11.5. All users have a responsibility to report immediately to ICT Technicians any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

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

5.11.7. The young people will be made aware of the importance of filtering systems through the e-safety education program. They will also be made aware of the consequences of attempting to subvert the filtering system.

5.11.8. Staff users will be made aware of the filtering systems through

5.11.8.1. Signing the AUA
5.11.8.2. Induction training
5.11.8.3. Staff meetings, briefings, INSET days.

5.11.9. Parents will be informed of the school's filtering policy through the Acceptable Use Agreement and through e-safety awareness sessions / newsletter etc.

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

5.11.10.1. The Technical Committee
5.11.10.2. Governors.

5.11.11. Filtering will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision.

5.11.12.

5.12.**School Password Security**

5.12.1. The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that:

5.12.1.1. Users can only access data to which they have right of access.
5.12.1.2. No user should be able to access another's files, without permission (or as allowed for monitoring purposes within the school's policies).
5.12.1.3. Access to personal data is securely controlled in line with the school's Personal Data Handling guidelines below.
5.12.1.4. Logs are maintained of access by users and of their actions while users of the system.

5.12.2. A safe and secure username and password system is essential if the above is to be established and will apply to all school ICT systems.

5.12.3. The management of password security will be the responsibility of the Network Manager and ICT Technicians.

5.12.4. All users will have responsibility for the security of their username and password must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security. Pupils will need the support of an adult to log on to their ipad or class computers. In these circumstances staff will have access to password details etc.

5.12.5. Passwords for new users and replacement passwords for existing users can be allocated by the Network Manager and the ICT Technicians.

5.12.6. Members of staff will be made aware of the school's password protocols:

5.12.6.1. At induction
5.12.6.2. Through the school's E-safety and password security protocols
5.12.6.3. Through the Acceptable Use Agreement

5.12.7. Young people will be made aware of the school's password protocols:

5.12.7.1. In ICT sessions and E-safety assemblies
5.12.7.2. Through the Acceptable Use Agreement

5.12.8. All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the Network Manager and will be reviewed by the Technical committee, when required.

5.12.9. All users will be provided with a username and password by the Network Manager and ICT Technicians who will keep an up to date record of users and their usernames.

5.12.10. The following rules apply to the use of passcodes:

5.12.10.1. The password for the Windows accounts will be the New Bridge passwords and are given to staff by the ICT Technicians.
5.12.10.2. The passcode for iPads will be a minimum of 4 digits.
5.12.10.3. Passwords shall not be displayed on screen, and shall be securely hashed.

5.12.11. The "administrator" passwords for the school ICT system, used by the Network Manager must also be available to the Head of Site or other nominated senior leader and kept in a secure place (eg school safe).

5.12.12. The Network manager and ICT Technicians will ensure that full records are kept of:

5.12.12.1. User Ids and requests for password changes
5.12.12.2. User log-ons
5.12.12.3. Security incidents related to ICT

5.12.13. In the event of a serious security incident, the police may request and will be allowed access to accounts.

5.12.14. User lists, IDs and other security related information must be given the highest security classification and stored in a secure manner.

5.13.**Personal Data Handling**

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

5.13.1.1. Have permission to access that data

5.13.1.2. Need to have access to that data.

5.13.2. Any loss of personal data can have serious effects for individuals and / or institutions concerned, can bring the school into disrepute and may well result in disciplinary action and / or criminal prosecution. All transfer of data is subject to risk of loss or contamination.

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

5.13.4. The Data Protection Act (2018) lays down a set of rules for processing of personal data. It provides individuals with rights of access and security and requires users of data to be open about how it is used and to follow the data protection principles.

5.13.5. All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation. The use of portable storage media such as USBs is not permitted.

5.13.6. Any Cloud service storing personal data must be GDPR compliant.

5.14. **Incidents of Misuse**

5.14.1. The school believes that the activities referred to in the chart shown at Appendix 4 be inappropriate in a school context and that users should not engage in these activities in school or outside school when using school equipment or systems.

5.15. **Responding to incidents of misuse**

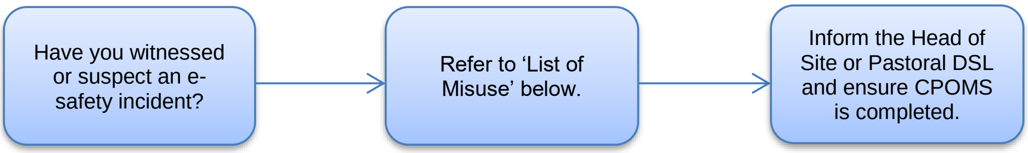
5.15.1. It is expected that all members of the school community will be responsible users of ICT. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

5.15.2. The flow chart (below) should be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.

5.16. **Incidents of Misuse**

5.16.1. It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. However, it is important that any incidents are dealt with as soon as possible.

5.16.2. The following process should be followed for reporting any e-safety incident:


Have you witnessed or suspect an e-safety incident?
Refer to 'List of Misuse' below.
Inform the Head of Site or Pastoral DSL and ensure CPOMS is completed.

Below is a list of actions by staff or young people that is considered misuse of technology.

	Misuse
Unacceptable and illegal misuse	Accessing or sharing child sexual abuse images
	Accessing or sharing adult material that breaches the Obscene Publication Act 2019
	Inciting racial or religious hatred
Unacceptable	Accessing pornographic material
	Threatening behaviour, including promotion of physical violence or mental harm
	Using school systems to run a private business
	Using school systems to bypass filtering
	Corrupting or destroying another person's data
	Uploading/downloading commercial software or any copyrighted materials without the necessary licensing permissions
	Sharing confidential information (eg financial / personal information, computer / network access codes and passwords)
	Creating or propagating computer viruses or other harmful files
	Online gambling
	Sending offensive/intimidating/ bullying messages
	Use of school email for personal emails
	Using personal accounts (email/social media/text, etc) to communicate with young people and parents
	Sharing photos or videos of pupils online
	Use of mobile phones during working time, unless in emergencies or for educational projects.
	Taking photos of pupils on personal devices/mobile phones.
Acceptable at certain times	Use of social media
	Use of personal email addresses
	Use of video broadcasting
	Use of mobile phones in social time
	Online gaming (non-educational)
	Online shopping
Acceptable	Use of iPads and tablets for educational purposes
	Online gaming (educational)
	Use of blogs for educational purposes

6. **Sources and references**
   6.1. Beyond the E-safety net – DFE guidance
   6.2. Safeguarding children in a digital world - DfE

7. **Other useful documents**
   7.1. Safeguarding Policy
   7.2. Anti-Bullying Policy
   7.3. Allegations of Abuse against Staff Policy
   7.4. Disciplinary Policy
   7.5. Behaviour Policy
   7.6. Code of Conduct for Staff

8. **Monitoring**
   8.1. This policy will be monitored through the Group's accountability framework.

Staff Acceptable Use Agreement **Appendix 1**

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

This Acceptable Use Agreement is intended to ensure:

- That staff will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- That school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- That staff are protected from potential risk in their use of ICT in their everyday work.
- The school will ensure that staff will have good access to ICT to enhance their work, to enhance learning opportunities for our young people and will, in return, expect staff to agree to be responsible users.

For my professional and personal safety:

a) I understand that the school will monitor my use of the ICT systems, email and other digital communications including personal devices that are connected to the network via wifi.
b) I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the rules set down by the school
c) I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
d) I will immediately report any illegal, inappropriate or harmful material or incident I become aware of to the appropriate person.
e) I will be professional in my communications and actions when using school ICT systems:
f) I will not access, copy, remove or otherwise alter any other user's files, without their permission.
g) I will communicate with others in a professional manner,
h) I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
i) I will ensure that when I take images of others I will do so with their permission and in accordance with the school's policy on the use of digital and video images. I will not use my personal equipment to record these images, in accordance with school's policy on the use of digital and video images. I will only use my school ipad.
j) I will only use chat and social media sites during unstructured times in school and in accordance with the school's policies. I will never accept a 'friends' request from a young person.
k) I will only communicate with young people and parents / carers using official school systems. Any such communication will be professional in tone and manner.
l) I understand that if I engage in any on-line activity it may compromise my professional responsibilities.
a) I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
b) I will ensure that my data is regularly backed up.
c) I will not upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others.
d) I will not use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.

e) I will not (unless I have permission) make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
f) I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.
g) I will not disable or cause any damage to school equipment, or the equipment belonging to others.
h) Where personal data is transferred outside the secure school network, it must be encrypted. Not use portable storage media such as USBs, and only use school-approved Cloud services which are GDPR compliant.
i) I understand that data protection policy requires that any staff or young person's data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by the school to disclose such information to an appropriate authority.
j) handle my school-provided iPad with care and respect at all times and never remove it from the protective case.
k) keep my iPad and laptop secure at all times, not leaving it unattended in my vehicle, and lock it away whenever it is not being used.
l) I will immediately report any damage or faults involving equipment or software however this may have happened.
m) not carry out repairs on any school-owned device, or solicit any individual or company to repair a school-owned device on my behalf.
n) attempt to remove my device from school's device management system and ensure my files are only backed up to my iCloud or to the New Bridge IT systems (staff drive/home drive).

When using the internet in my professional capacity or for school sanctioned personal use:
a) I will ensure that I have permission to use the original work of others in my own work
b) Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of school:
a) I understand that this Acceptable Use Agreement applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
b) I understand that if I fail to comply with this Acceptable Use Agreement, I could be subject to disciplinary action.

Staff name: ___________________________________

Signature: ____

Date: _________________