E-Safety Policy for

All Hallows Catholic School

Document Control

Date	Version	Changes	Senior Leadership Team Approval	Governing Body Approval
20 May 21	V1.0	Updated with new format	T Fanshawe & L Powell	Education & Standards Committee
7 Jun 23	V1.1	Updated for 2023/2024	D Hurley	Education & Standards Committee

Review Schedule:

Document Reference PPL.051

Review Cadence: Annual

Next review date: Jun 2024

Our School Vision

Our vision at All Hallows is to form happy, successful students who reach their full potential and leave the school with integrity and moral purpose. We want a whole school experience that everyone would wish for their own children. We put our students at the heart of everything we do, guided by the truth and love of Christ.

Introduction

Background / Rationale

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone.

Electronic communication helps teachers and students 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.

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.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote student 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:

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

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 our other school policies (e.g. Behaviour and Child Protection & Safeguarding Policies).

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

1. Key Personnel

Designated Safeguarding Leads (DSL(s) are: dsl@allhallows.net
Mr David Hurley - Contact details: d.hurley@allhallows.net, Tel: 01252 319211
Mr Chris Rees - Contact details: c.rees@allhallows.net, Tel: 01252 319211

Deputy DSL(s) are:
Head of Lower School: Mr Rob Antrobus - Contact details: r.antrobus@allhallows.net
Head of Upper School: Miss Vikki Milnes - Contact details: v.milnesl@allhallows.net
Special Education Needs and Disabilities Co-ordinator (SENDCo): Miss Rebecca Peters
Contact details: r.peters@allhallows.net
Lay Chaplain: Mrs Teresa Fanshawe - Contact details: t.fanshawe@allhallows.net

The nominated Child Protection/Safeguarding Governor is: **Mrs Anne Long**
Contact details: a.long@Governors.allhallows.net

The Headteacher is: **Mr Mark Baines**
Contact details: m.baines@allhallows.net

The Chair of Governors is: **Mr Ian Anderson**
Contact details: i.anderson@Governors.allhallows.net

2. Scope of the Policy

This Policy applies to all members of the school community (including staff, students, volunteers, parents/carers, visitors, community users) who have access to, and are users of, school technology systems, both in and out of school. The Education & Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

This is pertinent to incidents of cyber-bullying, or other e-policy & procedure safety incident covered by this Policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this Policy and associated Behaviour and Anti-Harassment & Anti-Bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of school.

3. Roles & Responsibilities

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

Governors:
Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the Policy. This will be carried out by the Governors/Governors Sub Committee receiving regular information about e-safety incidents and monitoring reports.

Headteacher & Senior Leaders:
The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the ICT lead - Miss L Powell.

- The Headteacher/Senior Leaders are responsible for ensuring that the ICT lead and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant
- The Headteacher/Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive annual monitoring reports from the ICT lead.
- The Headteacher and another member of the Senior Leadership Team/Senior Management Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

ICT Lead: Miss L Powell
- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies/documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provides training and advice for staff.
- Liaises with the Local Authority, if required.
- Liaises with school technical staff.
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
- Attends relevant meetings/committee of Governors, if requested.
- Reports annually to the Headteacher

Technical staff:
IT Technicians should ensure:
- That the school's ICT infrastructure is secure and is not open to misuse or malicious attack.
- That users may only access the school's networks password protected user accounts.
- That breaches in e-safety are monitored and reported to the ICT lead, Miss Powell as necessary.

Teaching and Support Staff
The teaching and support staff are responsible for ensuring that:
- They have an up-to-date awareness of e-safety matters and of the current school E-Safety Policy and practices.
- They have read, understood and signed the school Staff Acceptable Use Policy / Agreement.
- They report any suspected misuse or problem to the ICT lead or Headteacher for investigation.
- Digital communications with students (e-mail/ voice) should be on a professional level and only carried out using official school systems.
- E-safety issues are embedded in all aspects of the curriculum and other school activities.
- Students understand and follow the School e-safety and Acceptable Use Policy
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor ICT activity in lessons, extra-curricular and extended school activities
- They are aware of e-safety issues related to the use of mobile phones, cameras and handheld devices and that they monitor their use and implement current school policies regarding these devices
- In lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. They should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

- Staff are allowed to take digital / video images to support educational aims, but must follow school procedures concerning the sharing, distribution and publication of those images. If digital / video images are taken on personal devices these must be downloaded to the school network at the first opportunity and deleted from the device.
- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include students will be selected carefully. Staff should refer to the list of photographs of students which are not to be published. This list is available from Mrs Angela Denman.
- Students' full names can be used on a website if parents have given prior permission. Data Protection Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 (Data Protection Act 2018, which came into force from 25 May 2018), which states that personal data must be:
    - Fairly and lawfully processed
    - Processed for limited purposes
    - Adequate, relevant and not excessive
    - Accurate
    - Kept no longer than is necessary
    - Processed in accordance with the data subject's rights
    - Secure
    - Only transferred to others with adequate protection

Following a number of "high profile" losses of personal data by public organisations, schools are likely to be subject to greater scrutiny in their care and use of personal data.

The use of ICT and technological resources is in our everyday teaching routines. We use them often and do not always think about the day-to-day aspects of use. Every time we use our computers, we leave them open to abuse by other members of staff or even the children we teach. This Policy is to alter our day-to-day use of technology to protect our work and the confidential nature of some of our uses of technologies.

At times when not in use, Desktops should be locked and not be accessible by anyone. Desktop passwords should be confidential and not shared.

Staff Visitor's Use
The IT technician will provide a temporary password for visitors, when requested.

Staff Designated Safeguarding Lead (DSL)
The DSL should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:
- Sharing of personal data
- Access to illegal / inappropriate materials
- Inappropriate on-line contact with adults / strangers
- Potential or actual incidents of grooming
- Cyber-bullying

Students
- Are responsible for using the school ICT systems in accordance with the Student Acceptable Use Policy, which they will be expected to sign before being given access to school systems.
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

- Will be expected to know and understand school policies on the use of mobile phones, digital cameras and handheld devices. They should also know and understand school policies on the taking/use of images and on cyber-bullying.
- Should understand the importance of adopting good 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.

Parents/Carers

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 IT than their children.

The school will, therefore, take every opportunity to help parents understand these issues through parents' information evenings, newsletters, letters, website/information about national /local e-safety campaigns/literature.

Parents and carers will be responsible for:

- Endorsing the Student Acceptable Use Policy
- Accessing the school website / Student records in accordance with the relevant school Acceptable Use Policy

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in e-safety is therefore an essential part of the school's e-Safety provision. Children and young people need the help and support of the school to recognise and avoid e-Safety risks and build their resilience.

4. Policy E-Safety Education will be provided in the following ways:

- A planned e-safety programme should be provided as part of ICT/PSHE/other lessons and should be regularly revisited – this will cover both the use of current and new technologies in school and outside school. Teachers have been provided with suitable and age-appropriate planning for teaching e-safety. There is help and advice on the school website together with the wealth of information available to support the teaching of e-safety, some of which listed below:
    - www.thinkuknow.co.uk
    - www.saferinternet.org
    - www.childnet.com/cyberbullying-guidance
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities.
- Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Students should be helped to understand the need for the student AUP and encouraged to adopt safe and responsible use of technology, the internet and mobile devices both within and outside school.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Staff should act as good role models in their use of technology, the Internet and mobile devices.

5. Education - Parents/Carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's on-line experiences.

Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).

The school will therefore seek to provide information and awareness to parents and carers through:

- Parent's information evenings
- Letters
- Newsletters
- The web site

6. Education & Training

Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this Policy.

Training will be offered as follows:

- Some staff will identify e-safety as a training need within the performance management process.
- New staff will be able to access the E-Safety Policy and will be shown the acceptable use Policy/agreement at each login to the school network.
- This E-Safety Policy and its updates will be presented to and discussed by staff in staff / team meetings/INSET days.
- The ICT lead (or other nominated person) will provide advice / guidance / training as required to individuals as required.

Governors

Governors should take part in e-safety training/awareness meetings as required, with particular importance for those who are members of any sub-committee/group involved in ICT/ e-safety/health and safety/child protection.

This will be offered as individual training as required.

Technical – infrastructure/equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible, and that policies and procedures approved within this Policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities.

- 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 ICT support.
- All users will be provided with a username and password by the ICT support department who will keep an up to date record of users and their usernames.
- The administrator passwords for the school ICT system, used by ICT must also be available to the Headteacher and the ICT Lead.
- Users will be made responsible 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.
- Any filtering issues should be reported immediately to the ICT Lead or Headteacher.
- Requests from staff for sites to be removed from the filtered list will be considered by the Headteacher and this will be requested of the ICT support company for the specified amount of time.

Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data.

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

- In lessons, where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit. The use of Google Chrome and Bing allow for safer use of internet when searching images.
- Students should be taught in all lessons to be critically aware of the materials/ content they access on-line and be guided to validate the accuracy of information.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Use of digital and video images -Photographic, Video
The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees.

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:
- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. They should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites. Staff must not use personal devices to record pictures/images or videos on for school use.
- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images.
- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students are published on the school website. This is part of the school's paperwork that is completed for all new students on role.
- Students' work can only be published with the permission of the student and parents or carers. Data Protection "In the digital world strong cybersecurity and data protection go hand in hand. The 2018 Act is a key component of our work to secure personal information online,"

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 which states that data protection must be:
- Fairly and lawfully processed
- Fit for the digital age when an ever-increasing amount of data is being processed.
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Secure
- Only transferred to others with adequate protection

7. General Data Protection Regulations (GDPR) May 2018

Schools handle a large amount of personal data. This includes information on students, such as grades, medical information, images and much more. Schools also hold data on staff, Governors, volunteers and job applicants. Schools will also handle what the GDPR refers to as special category data, which is subject to tighter controls. This could be details on race, ethnic origin, biometric data or trade union membership.

To comply with the GDPR:

- The school has appointed a Data Protection Officer (DPO) - Caroline Antrobus
- Demonstrate compliance- schools need to document every system used to process personal data
- Processor agreements - for 3rd party processors contracts must be in place stipulating the handling of personal data in compliance with GDPR.
- Reporting a data breach- if personal data has been but at risk, it may be required that Surrey are informed, and in some cases the affected individual. There is a time frame of 72 hours in which this must be done from discovery of the breach
- Staff Training- making sure staff are trained and that data compliance is crucial, being that devices are only as secure as those using them.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse. Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.

8. Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning.

The official school e-mail service may be regarded as safe and secure and is monitored.

Staff and students should, therefore, use only the school e-mail service to communicate with others when in school, or on school systems (eg. by remote access). Staff should not use personal e-mails to communicate school matters.

- Users need to be aware that e-mail communications may be monitored.
- Users must immediately report to the nominated person – in accordance with the school Policy, the receipt of any e-mail that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such e-mail.
- Any digital communication between staff and students or parents/carers (e-mail, chat, Teams/SharePoint etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal e-mail addresses, text messaging or public chat/social networking programmes must not be used for these communications.
- All students will be provided with individual school e-mail addresses for educational use.
- Students should be taught about e-mail safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate e-mails and be reminded of the need to write e-mails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official e-mail addresses should be used to identify members of staff.

The use of Social Media

All adults working in school must always maintain professional conduct with students and their families. Communication with children and families must be limited to that required to discharge your professional duty. Staff must remember they are bound by confidentiality, so should ensure any communication is in the best interests of the school and its students. All Staff must present a professional front at all times, across all media formats, as we are the public face of the school.

Any social media groups, such as Twitter, which are linked to the school will be vetted and post deemed inappropriate will be removed.

School staff: All school staff are in a position of trust, and there are expectations that they will always act in a professional manner.

Key advice for staff to protect their online reputation:

- Ensure you understand the school's guidance on the use of social media.
- Do not leave electronic devices logged on when away from your desk. 'Lock' your computer should you need to leave it for a substantial amount of time.
- Enabling a password, that only you know, to log into your pc/ipad, ensures that personal details are kept secure.
- It is a good idea to keep a check on your online presence-Google yourself and see how secure your internet settings are online and also if there are negative comments it is easier to address as soon as it appears.

9. Unsuitable/Inappropriate Activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school Policy restricts certain internet usage as follows.

Staff and other adults

	Allowed	Allowed at certain times	Allowed to certain staff	Not allowed
Mobile phones may be brought to school	x			
Use of mobile phone in lesson				x
Use of personal e-mail address in school or on school network				x
Use of school e-mail for personal e-mails				x
Use of social networking sites				x
Taking photos on mobile phone				x
Use of blogs			x	

Students

	Allowed	Allowed at certain times	Allowed with staff permissio n	Not allowed
Mobile phones may be brought to school	x			
Use of mobile phone in lesson				x
Use of phone around school site				x
Use of personal e-mail address in school or on school network				x
Use of school e-mail for personal e-mails				x
Use of social networking sites				x

It is hoped that all members of the school community will be responsible users of technology, who understand and follow this Policy. However, there may be times when infringements of the Policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

Listed below are the responses that will be made to any apparent or actual incidents of misuse; if any apparent or actual misuse appears to involve purposeful illegal activity e.g:

- Child sexual abuse images
- Adult material which potentially breaches the Obscene Publications Act
- Criminally racist material
- Other criminal conduct, activity or materials

The Headteacher will be informed and will carry out a formal investigation which may involve other agencies eg. the Police or Social Services.

10. Cyber-Bullying

The use of the internet and social media has created further opportunities for bullying to take place. School leaders, teachers, staff, parents and students all have rights and responsibilities in relation to cyber-bullying and should work together to create an environment in which all can learn and develop and are free from harassment and bullying.

As a school, we discuss cyber-bullying as part of our PSHE and e-safety programme, what to do if it happens to them and who to report it to. We will support parents on how to help their children engage safely and responsibly with social media, through advice in the school newsletter or signposting to useful sources of support and advice. This will enable concerns to be raised in an atmosphere of trust and in an appropriate manner. We want our students, parents and staff to use social media responsibly and in a way that benefits all, but reminders should be made that this should be done within the correct context.

For further information see the publication 'Cyber-bullying advice for Headteachers and School Staff 121114' Published by the DfE 2014: ref- DFE-00652-2014

11. User Actions

	Acceptable	Not Acceptable
Users shall not: visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to those given. When 'acceptable' is indicated, the reasons for use must be for an educational purpose.		
Child sexual abuse images		X
Promotion or conduct of illegal acts eg. computer misuse and fraud		X
Adult material that potentially breaches the Obscene Publications Act in the UK		X
Criminally racist material in UK		X
Pornography		X
Promotion of any kind of discrimination		X
Promotion of racial or religious hatred		X
Threatening behaviour, including promotion of physical violence or mental harm		X
Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute		X
Using school systems to run a private business		X

Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school		x
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions		x
Revealing or publicising confidential or proprietary information (eg financial/personal information, databases, computer/network access codes and passwords)		x
Creating or propagating computer viruses or other harmful files		x
Carrying out sustained or instantaneous high volume network traffic (downloading/uploading files) that causes network congestion and hinders others in their use of the internet		x
On-line gaming (educational)	x	
On-line gaming (non-educational)		x
On-line gambling		x
On-line shopping/commerce for staff	x	
File sharing		x
Use of social networking sites by students		x