



HEREWARD HOUSE SCHOOL

## HEREWARD HOUSE SCHOOL

### E-Safety and Cyber Bullying Policy

---

Author: Pascal Evans

Policy ratified by: SMT

Date of publication: 30<sup>th</sup> October 2018

Date of next review: 30<sup>th</sup> October 2019

Governor responsible for policy: Alex Jenne

## **Hereward House School: e-Safety and Cyber Bullying Policy**

### **Our School's Aims**

At Hereward House we aim to provide a warm, welcoming and safe atmosphere in which every child can thrive and feel comfortable. Whilst embracing the highest academic aspirations for our boys, we believe that a school should not be an exam factory. We strive to create a stimulating, purposeful and happy community, where every child feels valued and secure. We aim to be a school where boys will be encouraged and assisted to develop academically, morally, emotionally, culturally and physically. It is our belief each one should enjoy his school days and reflect upon them with pride, pleasure and affection. We are preparing boys not just for senior school, but for life.

### **Introduction**

Hereward House School is committed to ensuring a warm, welcoming and safe atmosphere in which every child can thrive and feel comfortable. It is the school's duty to ensure every pupil in its care is safe; and the same principles apply to the digital world as apply to the real world. IT and online communications provide unrivalled opportunities for enhanced learning in addition to traditional methods, but also pose greater and more subtle risks to young people. Our pupils are therefore taught how to stay safe in the online environment and how to mitigate risks, including but not limited to, the risk of identity theft, bullying, harassment, grooming, stalking and abuse.

New technologies are continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. Current and emerging technologies used in and outside of school include:

- Websites;
- Email and instant messaging;
- Blogs;
- Social networking sites;
- Chat rooms;
- Music / video downloads;
- Gaming sites;
- Text messaging and picture messaging;
- Video calls;
- Podcasting;
- Online communities via games consoles; and
- Mobile Internet devices such as smart phones and tablets.

This policy is implemented to protect the interests and safety of the whole school community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements. It is linked to the following school policies:

- Safeguarding and Child Protection

## **Hereward House School: e-Safety and Cyber Bullying Policy**

- Behaviour, Rewards and Sanctions;
- Anti-Bullying;
- PSHEE.

Whilst exciting and beneficial both in and out of the context of education, much IT, particularly online resources, is not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Hereward House, we understand the responsibility to educate our pupils on e-safety issues; teaching them the appropriate behaviours and critical thinking skills necessary to enable them to remain both safe, and within the law, when using the Internet and related technologies in and beyond the classroom.

This policy covers both fixed and mobile Internet devices provided by the school (such as PCs, laptops, webcams, tablets, whiteboards, digital video equipment, etc.); as well as all devices owned by pupils and staff brought on to school premises (personal laptops, tablets, smart phones, etc.).

### **Roles and responsibilities**

The Designated Safeguarding Lead (DSL) and ICT manager have responsibility for ensuring this policy is upheld by all members of the school community. They will keep up to date on current e-safety issues and guidance issued by organisations such as the Local Authority, CEOP (Child Exploitation and Online Protection), Childnet International and the Local Authority Safeguarding Children Board. As with all issues of safety at this school, staff are encouraged to create a talking culture in order to address any e-safety issues which may arise in classrooms on a daily basis.

As part of the school's online safeguarding measures, it is the responsibility of the ICT Manager to ensure a strong Internet content filtering system is set up on all school technology accessing the Internet. It is also the responsibility of the ICT Manager to regularly check (and when necessary, update) the list of 'blocked sites' to ensure continued pupil online protection.

The school believes that it is essential for parents/carers to be fully involved with promoting e-safety both in and outside school. We regularly consult and discuss e-safety with parents/carers and seek to promote a wide understanding of the benefits and risks related to Internet usage. It is the responsibility of the ICT Manager to deliver e-safety advice talks to parents, educating parents on current online dangers, personal data safety tips, popular website and social media uses with each year group and tips for setting online security settings. E-safety advice material is also made accessible to parents via the school website, which, again, is the responsibility of the ICT Manager to keep updated each academic year.

## **Hereward House School: e-Safety and Cyber Bullying Policy**

### **Staff awareness**

New teaching staff receive information on personal e-safety and acceptable Internet use on school premises, as part of their induction. All teaching staff receive regular information and training on e-safety issues in the form of INSET training and internal meeting time, and are made aware of their individual responsibilities relating to the safeguarding of pupils within the context of e-safety.

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following school e-safety procedures. When pupils use school computers, staff should make sure they are fully aware of the agreement they are making to follow the school's IT guidelines.

Teaching staff are encouraged to incorporate e-safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. They should know what to do in the event of misuse of technology by any member of the school community.

If any incident relating to e-safety occurs it must be reported to the Deputy Head as soon as possible. If a staff member is concerned that the incident may be a safeguarding concern it must be reported directly to the school's DSL in line with the school's Safeguarding and Child Protection Policy.

### **E-Safety in the curriculum and school community**

IT and online resources are used increasingly across the curriculum. We believe it is essential for e-safety guidance to be given to pupils on a regular and meaningful basis. We continually look for new opportunities to promote e-safety and regularly monitor and assess our pupils' understanding of it.

The school builds resilience in its pupils by providing them with opportunities to learn about e-safety within a range of curriculum areas and ICT lessons. Educating pupils on the dangers of technologies that may be encountered outside school will also be carried out via PSHEE, as well as informally, when opportunities arise.

At age-appropriate levels, and usually via PSHEE or ICT, pupils are taught to look after their own online safety. Pupils are informally taught about recognising online sexual exploitation, stalking and grooming, the risks, and of their duty to report any such instances they or their peers come across. Pupils can report concerns to the DSL, their form teacher and any member of staff at the school.

Pupils are also taught about relevant laws applicable to using the Internet; such as data protection, intellectual property and legal age limits on certain Social Media websites and mobile apps. As part of the School's pupil 'Acceptable Internet Use Agreement' (please see

## **Hereward House School: e-Safety and Cyber Bullying Policy**

Appendix 1), pupils are taught about respecting other people's information and images (etc.) through discussion and classroom activities.

It is the responsibility of the ICT Manager to provide tailored e-safety advice talks to Forms 3-CE1, giving advice on safe searching online, appropriate website use, personal data safety tips and possible implications of inappropriate use of pupil photographs, the Internet, social media, or mobile communication technologies.

Pupils should be aware of the impact of cyber-bullying and know how to seek help, if they are affected by these issues (see also the school's Anti-bullying Policy). Pupils should approach the DSL and the Deputy as well as parents, peers and other school staff for advice or help if they experience problems when using the Internet and related technologies.

### **Use of school and personal technology devices**

#### **Staff**

School devices, assigned to a member of staff as part of their role must have a password or device lock so that unauthorised people cannot access the content. Staff should only use the school device, which is allocated to them for school work. When they are not using a device, staff should ensure that it is locked to prevent unauthorised access. Staff are not permitted to access inappropriate Internet sites on school, or personal technology devices, either in class or out of class. (The school's Internet content filtering system ensures this is possible). Any inappropriate use found will be reported directly to the school's DSL immediately and formal disciplinary actions will be imposed.

Staff are permitted to bring in personal devices for school related work use, however, no personal data should be projected onto interactive whiteboards in classrooms for pupils to see. A full virus scan must also be run on any personal technology, prior to connecting to the school server, every time it is used. It is the responsibility of the ICT manager (where possible) to ensure this is done. In the event that the ICT manager is unavailable, it is the responsibility of the Deputy Head to ensure this is done. If personal technology devices are used on School premises by staff, or visitors, no content or images related to pupils, should be stored on these personal technology devices at any time.

Staff may use their mobile telephone on school premises, but must do so out of sight of pupils, in the staff common room. Staff members are not allowed to use personal technology devices within the EYFS setting under any circumstances. All such equipment must be turned off and out of sight at all times in an EYFS setting.

Personal telephone numbers should not be shared with parents/carers and under no circumstances may staff contact a pupil using a personal telephone number.

## **Hereward House School: e-Safety and Cyber Bullying Policy**

### **Visitors**

Any visitors to the School may use a School or personal computer for school related work, while on School premises, though no access to the school server is to be granted and all internet access must be accessed via the school's internet content filtering system. Again, it is the responsibility of the ICT Manager to ensure this is done.

### **Pupils**

School mobile technologies available for pupil use including laptops, tablets, cameras, etc. are stored either in a locked cabinet or in the Deputy Head's office. Access is available via the Bursar or Deputy Head.

No personal devices belonging to pupils are to be used during lessons at school. Permission may be granted by the Headmaster for a pupil to use a personal laptop for typing in class. In such a scenario, all pupil devices must have a thorough virus scan run by the ICT Manager before allowing the device to be connected to the school network.

Any technology device used by pupils in school (school, or personal) will be granted limited access to the school network for security reasons. School devices used by pupils will be accessible via pupil logins, only allowing pupils to access the pupil network drive and the Internet, through a content filtering system.

Any attempt to access inappropriate content on a school, or personal technology device on school property will be reported directly to the Headmaster.

If pupils bring in mobile phones (e.g. for safety purposes if they walk to and from school alone), they should be kept switched off and left with their form teacher at the beginning of the school day. They may then be collected at the end of the school day.

### **Use of Internet and email**

#### **Staff**

Staff must not access social networking sites and any website or personal email which is unconnected with school work or business from school devices or whilst teaching or in front of pupils. Such access may only be made whilst out of sight of pupils.

When accessed from personal devices/off school premises, staff must use social networking sites with extreme caution, being aware of the nature of what is published online and its potential impact on their professional position.

There is strong anti-virus and firewall protection on our network and, as such, it may be regarded as safe and secure. Staff should be aware that email communications are monitored. All Internet use is filtered through an Internet content filtering system, which

## **Hereward House School: e-Safety and Cyber Bullying Policy**

runs on all staff computers. This restricts any access to websites deemed to contain inappropriate material.

Staff must immediately report to the Headmaster the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

Any online communications must not either knowingly or recklessly:

- place a child or young person at risk of harm;
- bring Hereward House School into disrepute;
- breach confidentiality;
- breach copyright;
- breach data protection legislation; or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
  - making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
  - using social media to bully another individual; or
  - posting links or material which is discriminatory, offensive, or inappropriate to pupils.

Under no circumstances should school pupils or parents be added as social network 'friends'.

Any digital communication between staff and pupils or parents/carers must be professional in tone and content. Under no circumstances may staff contact a pupil or parent/carer using a personal email address. The school ensures that staff have access to their work email address when offsite, for use as necessary on school business.

### **Pupils**

#### **Acceptable Internet Use Policy**

It is the responsibility of SMT and all teaching staff to ensure all pupils who access the Internet on school premises adhere to the pupil Acceptable Internet Use Policy, which outlines rules to adhere to when accessing the Internet and named websites/types of software pupils agree not to access on school premises.

There is strong anti-virus and firewall protection on our network. Spam emails, certain attachments and websites will be blocked automatically by the system. If this causes problems for school work/research purposes, pupils should contact the ICT manager for assistance.

Pupils should immediately report, to the Deputy Head or ICT Manager the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

## **Hereward House School: e-Safety and Cyber Bullying Policy**

Pupils must report any accidental access to materials of an inappropriate nature directly to the Deputy Head, ICT manager or another member of staff. Deliberate access to any inappropriate materials by a pupil will lead to the incident being recorded on their file and will be dealt with under the school's Behaviour, Rewards and Sanctions Policy. Pupils should be aware that all Internet usage via the school's systems and its Wi-Fi network is monitored.

### **Pupil's Online Safety – At School**

In line with the school's aim to provide a welcoming and safe atmosphere, in which every child can thrive and feel comfortable, the school takes online safeguarding extremely seriously. As part of the school's online safeguarding strategy, the school has a stringent Internet content filtering system in place, which restricts any access to websites deemed to contain inappropriate material. This filtering system is imposed on all technology (school, pupil, personal, or visitor's) accessing the Internet via the school's network.

It is the responsibility of the ICT Manager to ensure this content filtering system is set up on all school technology accessing the Internet. It is also the responsibility of the ICT Manager to regularly check (and when necessary, update) the list of 'blocked sites', to ensure continued pupil online protection.

### **Pupil's Online Safety - At Home**

Helpful e-Safety advice is given to all pupils from F3-CE1 each term, through eSafety ICT lessons, school assemblies and pupil e-Safety advice talks (mentioned in the E-Safety in the curriculum and school community section of this policy).

Several sites offer helpful advice to parents, particularly with respect to how they can best monitor their child's use of the computer at home. Important and useful information can be found on the following site:

[www.nextgenerationlearning.org.uk/safeguarding-learners/Safeguarding-learners-content/Parents-and-carers/](http://www.nextgenerationlearning.org.uk/safeguarding-learners/Safeguarding-learners-content/Parents-and-carers/).

### **Prevent Awareness**

Staff need to be aware of any pupils who may be in contact with or being targeted by violent extremists. Pupils are particularly at risk through use of internet and social media either at home or at school. Both the DSL and Governor with responsibility for safeguarding have undertaken Prevent awareness training. The school has a robust filtering system that ensure that pupils are safe from terrorist or extremist material when accessing the internet through the school system.

If there is evidence that a pupil is becoming deeply enmeshed in the extremist narrative, schools should seek advice from Camden's Integrated Youth Support Services on accessing



## **Hereward House School: e-Safety and Cyber Bullying Policy**

programmes to prevent radicalisation under the Channel project. Camden's Channel officer (0207 974 1475)

Although decisions to seek support for a child in need, or about whom there are concerns relating to radicalisation, would normally be taken in consultation with parents and pupils, their consent is not required for a referral when there are reasonable grounds to believe that a child is at risk of significant harm.

Further advice for staff and governors can be sought from the DfE dedicated helpline and mailbox: 020 7340 7264 and [counter-extremism@education.gsi.gov.uk](mailto:counter-extremism@education.gsi.gov.uk).

### **Data storage**

The school takes its compliance with the Data Protection Act 1998 seriously. Staff and pupils are expected to save all data relating to their work to the school's central server, where data backups are automatically made on a nightly basis.

Staff devices should be encrypted if any data or passwords are stored on them. The school expects all removable media (USB memory sticks, CDs, portable drives) taken outside school or sent by post or courier to be encrypted before sending.

Staff may only take information offsite when authorised to do so, and only when it is necessary and required in order to fulfil their role.

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the Deputy Head and ICT manager.

### **Password security**

Staff have individual school network logins, emails and storage folders on the server. Staff are regularly reminded of the need for password security.

All members of staff should:

- use a strong password (usually containing eight characters or more, and containing upper and lower case letters as well as numbers), which should be changed every 6 months;
- not write passwords down; and
- should not share passwords with pupils or staff.

### **Safe use of digital and video images**

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the Internet. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the Internet. Such images may

## **Hereward House School: e-Safety and Cyber Bullying Policy**

provide avenues for cyberbullying, stalking or grooming to take place. Digital images may remain available on the Internet forever and may cause harm or embarrassment to individuals in the short or longer term.

When using digital images, staff should inform and educate pupils 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 (e.g. on social networking sites).

In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published on blogs or social networking sites (etc.), nor should parents/carers comment on any activities involving other pupils in the digital/video images.

Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow this policy and the Safeguarding and Child Protection policy concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment: personal equipment should not be used for such purposes.

Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

Pupils must not take, use, share, publish or distribute images of others without their permission.

Written permission from parents or carers will be obtained before photographs of students/pupils are published on the school website.

Photographs published on the school website, or displayed elsewhere, that include pupils, will be selected carefully and will comply with good practice guidance on the use of such images. Pupils' full names will not be used anywhere on a website or blog if used in association with photographs.

### **Cyber-Bullying**

Central to the School's anti-bullying procedure is the belief that bullying is not tolerated in any form. This includes through electronic communication either inside or outside of school. Under powers granted by the EIA 2006, Hereward House School is able to police cyber-bullying or any bullying aspects carried out by pupils even at home.

### **Definition of Cyber-Bullying**

Updated 9<sup>th</sup> October 2018. Review October 2019

## **Hereward House School: e-Safety and Cyber Bullying Policy**

Cyber-bullying is an aggressive, intentional act carried out by a group or individual using electronic forms of contact repeatedly over time against a victim who cannot easily defend himself/herself.

By cyber-bullying, we mean bullying by electronic media:

- Bullying by texts or messages or calls on mobile phones
- The use of mobile phone cameras to cause distress, fear or humiliation
- Posting threatening, abusive, defamatory or humiliating material on websites, to include blogs, personal websites, social networking sites
- Using e-mail to message others
- Hijacking/cloning e-mail accounts
- Making threatening, abusive, defamatory or humiliating remarks in chat rooms, or on Social Media websites to include Facebook, Instagram, Youtube and Ratemymteacher

### **Legal Issues**

There is not a specific law which makes cyberbullying illegal but it can be considered a criminal offence under several different acts including Protection from Harassment Act (1997), Malicious Communications Act (1988), Communications Act (2003) Obscene Publications Act (1959) and Computer Misuse Act (1990).

### **Policy**

Hereward House School educates its pupils both in the proper use of telecommunications and about the serious consequences of cyber-bullying and will, through PSHEE and in ICT lessons and assemblies, continue to inform and educate its pupils in these fast changing areas.

The school trains its staff to respond effectively to reports of cyber-bullying or harassment and has systems in place to respond to it. The school endeavours to block access to inappropriate web sites, using firewalls, antivirus protection and filtering systems and no pupil is allowed to work on the Internet without a member of staff present. Where appropriate and responsible, the school audits ICT communications and regularly reviews the security arrangements in place.

Whilst education and guidance remain at the heart of what we do, the school reserves the right to take action against those who take part in cyber-bullying.

All bullying is damaging but cyber-bullying and harassment can be invasive of privacy at all times. These acts may also be criminal acts.

- The school supports victims and, when necessary, will work with the Police and CEOP (Child Exploitation and Online Protection) to detect those involved in criminal acts.

## **Hereward House School: e-Safety and Cyber Bullying Policy**

- The school will use, as appropriate, the full range of sanctions to correct, punish or remove pupils who bully fellow pupils or harass staff in this way, both in or out of school.
- The school will use its power of confiscation where necessary to prevent pupils from committing crimes or misusing equipment.
- All members of the School community are aware they have a duty to bring to the attention of the Headmaster any example of cyber-bullying or harassment that they know about or suspect.

### **Guidance for Staff**

If you suspect or are told about a cyber-bullying incident, follow the protocol outlined below:

#### **Mobile Phones**

- Ask the pupil to show you the mobile phone.
- Note clearly everything on the screen relating to an inappropriate text message, image, or social media post, to include the date, time and names.
- Take a screen shot photograph of the inappropriate material displayed on screen.
- Make a transcript of a spoken message, again record date, times and names.
- Tell the pupil to save the message/image.
- Go with the pupil and see the Headmaster, Deputy Head or in their absence, a member of the SMT.

#### **Computers**

- Ask the pupil to get up on-screen the material in question.
- Ask the pupil to save the material.
- Print off the offending material straight away.
- Make sure you have got all pages in the right order and that there are no omissions.
- Accompany the pupil, taking the offending material with you, to see the Headmaster or Deputy Head.
- Normal procedures for interviewing pupils and taking statements will then be followed particularly if a safeguarding issue is presented.

### **Guidance for Parents**

It is vital that parents and the school work together to ensure that all pupils are aware of the serious consequences of getting involved in anything that might be seen to be cyber-bullying. The school informs parents of the cyber-bullying policy and the procedures in place to deal with cyber-bullying. The school also provides yearly safety talks for parents in Forms 3-CE1,

## **Hereward House School: e-Safety and Cyber Bullying Policy**

outlining the school's policies on pupil's Internet use and providing safety tips to keep their son safe online.

- Parents can help by making sure their child understands the school's policy and, above all, how seriously the school takes incidents of cyber-bullying.
- Parents are given the option of signing a 'Parent/Child Agreement' which they can read through together, deciding on their own terms and conditions for online use at home and at school. (See Appendix 2)
- Parents should also explain to their sons legal issues relating to cyber-bullying.
- If parents believe their child is the victim of cyber-bullying, they should save the offending material (if need be by saving an offensive text on their or their child's mobile phone) and make sure they have all relevant information before deleting anything.
- Parents should contact the Headmaster as soon as possible. A meeting can then be arranged with the Headmaster, which may involve other relevant members of staff
- If the incident falls during the holidays, the school reserves the right to take action against bullying, perpetrated outside the school, which spills over into the school.
- Parents are encouraged to report/encourage their son to report any inappropriate content found, or inappropriate website behaviour to CEOP, using their 'report' button on the website: <https://www.ceop.police.uk/Ceop-Report/>.

### **Guidance for Pupils**

In addition to regular safety ICT lessons, the school also provides regular safety assemblies/talks to educate its pupils on legal issues of Internet usage, the dangers of using certain websites/social media and tips for personal data protection and safe use of the Internet.

- If you believe you or someone else is the victim of cyber-bullying, you must speak to an adult as soon as possible. This person could be a parent/guardian, your tutor, or the Headmaster.
- Do not answer abusive messages but log and report them.
- Do not delete anything until it has been shown to your Form Teacher, parents/guardian or the Headmaster (even if it is upsetting, the material is important evidence which may need to be used later as proof of cyber-bullying.)
- Do not give out personal IT details.
- Never reply to abusive e-mails.
- Never reply to someone you do not know.
- Always stay in public areas in chat rooms.

### **Complaints**

As with all issues of safety at Hereward House School, if a member of staff, a pupil or a parent/carer has a complaint or concern relating to e-safety prompt action will be taken to deal with it. Complaints should be addressed to the Headmaster (DSL) in the first instance,

## **Hereward House School: e-Safety and Cyber Bullying Policy**

who will undertake an immediate investigation and liaise with the leadership team and any members of staff or pupils involved. Please see the Complaints Policy for further information.

E-Safety and cyber bullying issues relating to safeguarding and child protection will be addressed by the Headmaster in his role as DSL, acting in accordance with the school's Safeguarding and Child Protection Policy.

### **National Bodies**

Further support and guidance may be obtained from the following:

[www.teachernet.gov.uk/wholeschool/behaviour/tacklingbullying/cyber-bullying](http://www.teachernet.gov.uk/wholeschool/behaviour/tacklingbullying/cyber-bullying)

[www.bullying.co.uk](http://www.bullying.co.uk)

The following information can be downloaded from the above website:

Safe to Learn: *Embedding anti-bullying work in schools* (2007):

- Cyber-bullying Guidance and Resources. Safe to Learn
- Cyber-bullying Summary Leaflet

[www.antibullying.net/cyber-bullying1.htm](http://www.antibullying.net/cyber-bullying1.htm) for an Information Sheet for Teachers and other Professionals who work with Young People

[www.becta.org.uk](http://www.becta.org.uk) for information on safeguarding learners

Beatbullying Anti-Bullying Alliance

Rochester House National Children's Bureau

4 Belvedere Road 8 Wakley Street

London London

SE19 2AT EC1V 7QE

020 8771 3377 020 7843 1901

[www.beatbullying.org](http://www.beatbullying.org) [www.anti-bullyingalliance.org.uk](http://www.anti-bullyingalliance.org.uk)

[https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/177099/D FE-00004-2012.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/177099/D FE-00004-2012.pdf)

## **Hereward House School: e-Safety and Cyber Bullying Policy**

### **Appendix 1**

#### **Acceptable Internet Use Agreement**

The school maintains computers and Internet access to help our learning. The rules you agree to follow in this agreement will keep everyone safe and help us to be fair to others.

- I will ask permission from a member of staff before using the Internet;
- I will not access another person's files without that person's permission;
- I will use the computers only for school work and homework;
- I will only e-mail people I know, or who my teacher has approved;
- The messages I send will be polite and sensible;
- I will not take, use or publish pictures of other people without their permission;
- I will not give my home address or phone number, or arrange to meet someone, unless my parent or teacher has given permission;
- To help protect other pupils and myself, I will tell a teacher if I see anything I am unhappy with or I receive messages I do not like;
- I understand that the school may check my computer files and may monitor the Internet sites I visit;
- I will not bring the school into disrepute when using social media and the Internet off site. I will be careful to avoid any behaviour that might be construed as bullying, including the deliberate exclusion of boys from online group conversations.

## **Hereward House School: e-Safety and Cyber Bullying Policy**

### **Appendix 2**

#### **Parent / Child Agreement**

It is my goal to use the Internet in a manner that is safe and responsible. I know that my online actions reflect the kind of person I am. The following are my personal standards for online activities.

I will protect my personal privacy by:

I will protect my personal reputation by:

I will treat others online in the following way:

The kind of sites and activities I will avoid include:

If I am communicating with someone I do not know in person, the steps I will take to make sure this person is safe are:

If I become worried that someone I am communicating with online is not safe (to me or to other children), I will:

The following are the steps I will take to keep myself safe if I ever want to meet an online stranger in person:

If I receive a communication from someone that is inappropriate or upsetting, I will:

If someone treats me badly online, including sending repeated inappropriate messages, or posting material elsewhere that damages my reputation or friendships, I will:

The amount of time that I will spend online during a typical day is:

The strategies I will use to ensure my online activities do not interfere with homework and other important tasks are:

If I see material posted online that makes me worried that someone else might be in danger, or might cause harm to others, I will:

I will ask you for assistance if:

Other commitments I make are: