E-Safety/Online Safety Policy

1. Aim of this policy

Wellacre Academy believes that online safety (e-Safety) is an essential element of safeguarding children and adults in the digital world, when using technology such as computers, mobile phones or games consoles.

The School identifies that the internet and information communication technologies are an important part of everyday life so children must be supported to be able to learn how to develop strategies to manage and respond to risk so they can be empowered to build resilience online.

The School has a duty to provide the school community with quality Internet access to raise education and standards, promote student achievement, support the professional work of staff and enhance the schools management functions. The School also identifies that with this, there is a clear duty to ensure that children are protected from potential harm online.

The purpose of this E- Safety Policy is to:

1) Clearly identify the key principles expected of all members of the school community with regards to the safe and responsible use of technology so that the School is a safe and secure environment.

2) Safeguard and protect all members of the School community online.

3) Raise awareness with all members of the School community regarding the potential risks as well as benefits of technology.

4) Enable all staff to work safely and responsibly, to model positive behaviour online and be aware of the need to manage their own standards and practice when using technology.

5) Identify clear procedures to use when responding to online safety concerns.

This policy applies to all staff and visitors including the governing body, and other individuals who work for, or provide services on behalf of the school as well as students, parents and carers.

This policy applies to all access to the internet and use of information communication devices including personal devices or where students, staff or other individuals have been provided with school issued devices for use off-site, such as a work laptop or mobile phone.

This policy must be read in conjunction with other relevant school policies including (but not limited to) Safeguarding and Child Protection, Anti-bullying, Behaviour for Learning, Home School Agreement, Data Protection policy, ICT acceptable Use policies (Staff and Student) Legislation and guidance.

2. Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on students' electronic devices where they believe there is a 'good reason' to do so.

Reducing online risks

The School is aware that the Internet is a constantly changing environment with new apps, tools, devices, sites and material emerging at a rapid pace. Emerging technologies will be examined for educational benefit and the Academy Leadership Team (ALT) will ensure that appropriate risk assessments are carried out before use in school is allowed. The School will ensure that appropriate filtering systems are in place to prevent staff and students from accessing unsuitable or illegal content.

The School will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer or device.

The School will audit technology use to establish if the Online Safety policy is adequate and that the implementation of the policy is appropriate.

Methods to identify, assess and minimise online risks will be reviewed regularly by the ALT.

Filtering decisions, internet access and device use by students and staff will be reviewed regularly by the ALT.

3. Roles and responsibilities

3.1 The governing body

The governing board has overall responsibility for monitoring this policy and holding the Principal to account for its implementation.

The designated governor for safeguarding will co-ordinate meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (Appendix 1)

3.2 The Principal

The Principal is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 Key responsibilities of the Designated Safeguarding Lead (DSL) are:

- Acting as a named point of contact on all online safety issues and liaising with other members of staff and agencies as appropriate.
- Keeping up-to-date with current research, legislation and trends.
- Coordinating participation in local and national events to promote positive online behaviour,
- Taking responsibility for online safety incidents and liaising with external agencies as appropriate.
- Regularly reviewing online safety incident logs and using them to inform and shape future practice.
- Ensuring all members of staff receive regular, up-to-date and appropriate training regarding online safety roles and responsibilities and provide guidance regarding safe appropriate communications.
- Ensuring that online safety is promoted to parents/carers and the wider community through a variety of channels and approaches.
- Work with the school's lead for data protection and data security to ensure that practice is in line with legislation.
- Maintaining an online safety incident/action log via CPOMS to record incidents and actions taken as part of the schools safeguarding recording structures and mechanisms.
- Monitor the school's e-safety incidents to identify gaps/trends and update the education response to reflect need and to report to the ALT, Governing Body and other agencies as appropriate.
- Liaising with the local authority and other local and national bodies as appropriate.
- Reviewing and updating online safety policies, Acceptable Use Policies for staff and students and other procedures on a regular basis (at least annually).
- Ensuring that online safety is integrated with other appropriate school policies and procedures.

3.4 Key responsibilities of staff are:

- Reading the School's Acceptable Use Policies and adhering to them.
- Taking responsibility for the security of school/ systems and data.
- Having an awareness of online safety issues, and how they relate to the children in their care.
- Modelling good practice in using new and emerging technologies
- Embedding online safety education in curriculum delivery wherever possible.
- Identifying individuals of concern, and taking appropriate action by working with the DSL.
- Knowing when and how to escalate online safety issues, internally and externally.
- Being able to signpost to appropriate support available for online safety issues, internally and externally.
- Maintaining a professional level of conduct in their personal use of technology, both on and off site.
- Taking personal responsibility for professional development in this area.
- Complete annual e-safety CPD
- Developing and promoting the online safety vision and culture to all stakeholders in line with national and local best practice recommendations with appropriate support and consultation throughout the school community.
- To read and sign the School's Acceptable Use Policies before using any school ICT resources.

Managing staff email

- All members of staff are provided with a specific school email address to use for any official communication.
- The use of personal email addresses by staff for any official school business is not permitted.
- The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains any content which could be subject to data protection legislation must only be sent using secure and encrypted methods.
- Sensitive or personal information will only be shared via email in accordance with data protection legislation.
- Access in school to external personal email accounts and social media may be blocked.
- School email addresses and other official contact details will not be used for setting up personal social media accounts.
- Email sent to external organisations should be written carefully before sending, in the same way as a letter written on school headed paper would be.
- Staff should never use their personal email or social media accounts to contact students.

3.5 Additional responsibilities for staff managing the technical environment are:

- Providing a safe and secure technical infrastructure which support safe online practices while ensuring that learning opportunities are still maximised.
- Taking responsibility for the implementation of safe security of systems and data in partnership with ALT.
- To ensure that suitable access controls and encryption is implemented to protect personal and sensitive information held on school-owned devices.
- Ensuring that the schools filtering policy is applied and updated on a regular basis and that responsibility for its implementation is shared with the DSL.
- Ensuring that the use of the School's network is regularly monitored in order that any deliberate or accidental misuse can be reported as necessary.
- Report any breaches or concerns to the DSL and ALT and together ensure that they are recorded on the on CPOMS, and appropriate action is taken as advised.
- Developing an understanding of the relevant legislation as it relates to the security and safety of the technical infrastructure.
- Report any breaches and liaising with the local authority (or other local or national bodies) as appropriate on technical infrastructure issues.
- Providing technical support and perspective to the ALT, especially in the development and implementation of appropriate online safety policies and procedures.
- Ensuring that the school's ICT infrastructure/system is secure and not open to misuse or malicious attack.
- Ensuring that appropriate anti-virus software and system updates are installed and maintained on all setting machines and portable devices.
- Ensure that appropriately strong passwords are applied and enforced.
- Maintain a current record of all staff and students who are granted access to the School's electronic communications.

3.6 Key responsibilities of students are:

- Students will read and sign the School's Acceptable Use Policies before using any school ICT resources and adhere to them.
- Respecting the feelings and rights of others both on and offline.
- Seeking help from a trusted adult if any concerns arise, and supporting others that may be experiencing online safety issues.
- Taking responsibility for keeping themselves and others safe online.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.

- Assessing the personal risks of using any particular technology, and behaving safely and responsibly to limit those risks.

Managing Student Email

- Students may only use school provided email accounts for educational purposes.
- Students must immediately tell a member of staff if they receive offensive or concerning communication.
- Access in school to external personal email accounts and social media may be blocked.
- School email addresses and other official contact details will not be used for setting up personal social media accounts.
- Students should only communicate with staff via their school email account and should not use their personal email account

3.7 Key responsibilities of parents/carers are:

- Reading the School's Acceptable Use Policy, encouraging their children to adhere to them, and adhering to them themselves where appropriate.
- Discussing online safety issues with their children, supporting the School in their online safety approaches, and reinforcing appropriate safe online behaviours at home.
- Role modelling safe and appropriate uses of new and emerging technology.
- Identifying and reporting to the School, or other appropriate agencies changes in behaviour that could indicate that their child is at risk of harm online.
- Seeking help and support from the School, or other appropriate agencies, if they or their child encounters online problems or concerns.
- Contributing to the development of the School's online safety policies.
- Using the School's systems, and other network resources, safely and appropriately.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- To read the School's Acceptable Use Policies for student access and discuss it with their child, where appropriate.

3.8 All external staff and volunteers

All external staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 1), and ensuring that students follow the school's terms on acceptable use (appendix 2)
- Working with the DSL to ensure that online safety incidents are able to be logged via CPOMS

This list is not intended to be exhaustive.

3.9 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (Appendix 1).

4. Educating students about online safety

Students will be taught about online safety as part of the RESPECT, SMSC and Computing curriculum. This will include:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, age restrictions, contact and conduct, and know how to report concerns
- Understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How content can be used and shared, online targeting and persuasive design
- Recognising Disinformation, misinformation, hoaxes, fake websites and online scams, including fraud and phishing scams
- Impact of social media on mental health
- How to recognise and report a range of concerns including abuse, online challenges, content that incites, fake profiles, grooming and inappropriate content
- Understand how to prevent and report cyberbullying
- The safe use of social media and the internet will also be covered in other subjects where relevant.
- The school will use assemblies to raise students' awareness of the dangers that can be encountered online and may also invite speakers to talk to students about this.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, via our website, social media accounts and via Parent Information evenings. This policy will also be shared with parents via the school website.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with their son's Achievement Tutor or DSL.

Concerns or queries about this policy can be raised with the DSL or Principal.

6. Appropriate and safe classroom use of the internet and associated devices

- The School's internet access will be designed to enhance and extend education.
- Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of students.
- Students will use appropriate tools to search the Internet for content.
- Internet use is a key feature of educational access and all children will receive age and ability appropriate education to support and enable them to develop strategies to respond to concerns as part of an embedded whole school curriculum.
- The School will ensure that the use of Internet-derived materials by staff and students complies with copyright law and acknowledge the source of information.
- All members of staff are aware that they cannot rely on filtering alone to safeguard students and supervision, classroom management and education about safe and responsible use is essential.
- Students will be appropriately supervised when using technology, according to their ability and understanding.
- All school owned devices will be used in accordance with the School's Acceptable Use Policy and with appropriate safety and security measures in place.

- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- The School will use the internet to enable students and staff to communicate and collaborate in a safe and secure environment.
- Students will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.

7. Cyber-bullying

7.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. The imbalance of power can manifest itself in several ways, it may be physical, psychological (knowing what upsets someone), derive from an intellectual imbalance, or by having access to the support of a group, or the capacity to socially isolate. It can result in the intimidation of a person or persons through the threat of violence or by isolating them either physically or online

(See also the school Behaviour for Learning and Anti Bullying policies.)

7.2 Responding to concerns regarding cyberbullying

- Cyberbullying, along with all other forms of bullying, of any member of the School's community will not be tolerated. Full details are set out in the school policies regarding anti-bullying and behaviour.
- All incidents of online bullying reported will be recorded.
- There are clear procedures in place to investigate incidents or allegations and support anyone in the school affected by online bullying.
- If the school is unclear if a criminal offence has been committed then the DSL will obtain advice immediately through appropriate agencies and/or Greater Manchester Police.
- Students, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The School will take steps to identify the bully. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Students, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the schools e-Safety ethos.
- Sanctions for those involved in online or cyberbullying may include:

    - Those involved will be asked to remove any material deemed to be inappropriate or offensive.
    - A service provider may be contacted to remove content if those involved refuse to or are unable to delete content.
    - Internet access may be suspended at school for the user for a period of time. Other sanctions for students and staff may also be used in accordance to the schools anti-bullying, behaviour policy or Acceptable Use Policies.
    - Parent/carers of students involved will be contacted
    - The police will be contact if a criminal offence has been committed.

7.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete

inappropriate images or files on students' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm
- Disrupt teaching
- Break any of the school rules, in particular breaches of the ICT Acceptable Use Policy

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the Academy Leadership Team to decide whether they should:

- Delete that material
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of students will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on students' electronic devices will be dealt with through the school complaints procedure.

8. Acceptable use of the internet in school

All students, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (Appendices 1 and 2). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by students, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1 and 2.

9. Students using mobile devices in school

The school has a no mobile device policy which is clearly communicated to all students, parents and carers. If a device is seen or heard it will be confiscated and stored securely in line with policy until it is returned at the end of the day when the students has served a detention for breach of policy.

See Mobile Device section of the Behaviour for Learning Policy.

10. Staff using work devices outside school.

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in Appendix 1.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

Work devices must be used solely for work activities.

11. Responding to Online Incidents and Concerns

- All members of the School community will be informed about the procedure for reporting online safety (e-Safety) concerns (such as breaches of filtering, cyberbullying, illegal content etc.).
- The DSL will be informed of any online safety (e-Safety) incidents involving child protection concerns, which will then be recorded.
- The DSL will ensure that online safety concerns are escalated and reported to relevant agencies.
- Complaints about online bullying will be dealt with under the School's Anti-bullying Policy
- Any complaint about staff misuse will be referred to the Principal
- Any allegations against a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community on a regular basis.
- The School will manage e-Safety incidents in accordance with the school Behaviour for Learning policy where appropriate.
- The School will inform parents/carers of any incidents of concerns as and when required.
- After any investigations are completed, the School will debrief, identify lessons learnt and implement any changes as required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the School will contact the TRAFFORD CHILDREN'S FIRST RESPONSE or Greater Manchester Police via 999 if there is immediate danger or risk of harm.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Greater Manchester Police.
- If the School is unsure how to proceed with any incidents of concern, then the incident will be referred to an appropriate external agency.
- Parents and children will need to work in partnership with the school to resolve issues.

11.1 Procedures for Responding to Specific Online Incidents or Concerns

Responding to concerns regarding Self-Generated Indecent Images of Children (SGIIOC or "Sexting")

- The School ensures that all members of the School are made aware of the social, psychological and criminal consequences of sharing, possessing and creating indecent images of children (known as "sexting").
- The School will implement preventative approaches via a range of appropriate educational approaches for students, staff and parents/carers.
- The School views "sexting" as a safeguarding issue and all concerns will be reported to and dealt with by the DSL.
- If the School is made aware of incident involving indecent images of a child the School will:

    - Act in accordance with the School's Safeguarding and Child Protection Policy and Trafford Strategic Safeguarding Board procedures.
    - Immediately notify the Designated Safeguarding Lead.
    - Store the device securely.
    - Carry out a risk assessment in relation to the children(s) involved.
    - Consider the vulnerabilities of children(s) involved (including carrying out relevant checks with other agencies)
    - Make a referral to children's social care and/or the police (as needed/appropriate).

- Put the necessary safeguards in place for children e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.
- Inform parents/carers about the incident and how it is being managed.
- Implement appropriate sanctions in accordance with the School's Behaviour for Learning policy but taking care not to further traumatise victims where possible.
- Review the handling of any incidents to ensure that the school is implementing best practice and the leadership team will review and update any management procedures where necessary.
- The School will not view the image unless there is a clear need or reason to do so.
- The School will not send, share or save indecent images of children and will not allow or request children to do so.
- If an indecent image has been taken or shared on the school/settings network or devices then the School will take action to block access to all users and isolate the image.
- The School will need to involve or consult the police if images are considered to be illegal.
- The School will take action regarding indecent images, regardless of the use of school equipment or personal equipment, both on and off the premises.
- The School will ensure that all members of the community are aware of sources of support.

11.2 Responding to concerns regarding Online Child Sexual Abuse

- The School will ensure that all members of the School are made aware of online child sexual abuse, including exploitation and grooming, including the consequences, possible approaches which may be employed by offenders to target children and how to respond to concerns.
- The School will implement preventative approaches for online child sexual abuse via a range of appropriate educational approaches for students, staff and parents/carers.
- The School views online child sexual abuse as a safeguarding issue and all concerns will be reported to and dealt with by the DSL.
- If the School is unclear if a criminal offence has been committed then the DSL will obtain advice immediately through TRAFFORD CHILDREN'S FIRST RESPONSE and/or Greater Manchester Police.
- If the school is made aware of incident involving online child sexual abuse of a child then the School will:

    - Act in accordance with the School's Safeguarding and Child Protection Policy
    - Immediately notify the DSL.
    - Store any devices involved securely.
    - Immediately inform Greater Manchester police via 101 (using 999 if a child is at immediate risk)
    - Where appropriate the School will involve and empower children to report concerns regarding online child sexual abuse.
    - Carry out a risk assessment which considers any vulnerabilities of student(s) involved (including carrying out relevant checks with other agencies).
    - Make a referral to children's social care (if needed/appropriate).
    - Put the necessary safeguards in place for student(s) e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.
    - Inform parents/carers about the incident and how it is being managed.
    - Review the handling of any incidents to ensure that the school is implementing best practice and the School's ALT will review and update any management procedures where necessary.
    - The School will take action regarding online child sexual abuse regardless of the use of school equipment or personal equipment, both on and off the school premises.
    - The School will ensure that all members of the School are aware of sources of support regarding online child sexual abuse.
    - If students at other schools are believed to have been targeted then the School will seek support from the TRAFFORD CHILDREN'S FIRST RESPONSE and the other

schools involved to enable other schools to take appropriate action to safeguarding their community.

11.3 Responding to concerns regarding Indecent Images of Children (IIOC)

- The School will ensure that all members of the School are made aware of the criminal nature of Indecent Images of Children (IIOC) including the possible consequences.
- The School will take action regarding IIOC regardless of the use of school equipment or personal equipment, both on and off the premises.
- The school will take action to prevent access accidental access to IIOC for example using an appropriate web filtering software, implementing firewalls and anti-spam software.
- If the School is unclear if a criminal offence has been committed then the DSL will obtain advice immediately through TRAFFORD CHILDREN'S FIRST RESPONSE and/or Greater Manchester Police.
- If the school/setting are made aware of IIOC then the School will:

    - Act in accordance with the School's Child Protection and Safeguarding Policy.
    - Immediately notify the School's DSL.
    - Store any devices involved securely.
    - Immediately inform appropriate organisations – Greater Manchester police via 101 (using 999 if a student is at immediate risk) and/or the Local Authority Designated Office (LADO) (if there is an allegation against a member of staff).

- If the school are made aware that a member of staff or a student has been inadvertently exposed to IIOC whilst using the internet then the School will:

    - Ensure that the DSL is informed.
    - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
    - Ensure that any copies that exist of the image, for example in emails, are deleted.

- If the School are made aware that IIOC have been found on the School's electronic devices then the school will;

    - Ensure that the DSL is informed.
    - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
    - Ensure that any copies that exist of the image, for example in emails, are deleted.
    - Inform the police via 101 (999 if there is an immediate risk of harm) and children's social services (as appropriate).
    - Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.

- If the School are made aware that a member of staff is found in possession of IIOC on their electronic device provided by the School, then the School will:

    - Ensure that the DSL is informed or another member of staff in accordance with the School's whistleblowing procedure.
    - Contact the police regarding the images and quarantine any devices involved until police advice has been sought.
    - Inform the LADO and other relevant organisations in accordance with the schools managing Allegations of Abuse against Staff policy.
    - Follow the appropriate school policies regarding conduct.

11.4 Responding to concerns regarding radicalisation or extremism online

- The School will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in school and that suitable filtering is in place which takes into account the needs of students.
- When concerns are noted by staff that a child may be at risk of radicalisation online then the DSL will be informed immediately and action will be taken in line with the School's Safeguarding and Child Protection Policy.

11.5 Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation as part of the safeguarding and Child Protection CPD package.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails and staff meetings).

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Staff will receive regular training on Cyber Security.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety via CPOMS. This policy will be reviewed annually by the Principal. At every review, the policy will be shared with the governing board.

13. Links with other policies

This online safety policy is linked to our:

- Safeguarding and Child Protection Policy
- Behaviour for Learning Policy
- Staff Disciplinary Procedures
- Data Protection Policy and Privacy Notices
- Complaints Procedure
- Dealing with Allegations of Abuse and Concerns Against Staff and Others Policy
- ICT Acceptable Use Agreement (staff and students)
- Anti-bullying Policy
- Social Media Policy
- Data Protection Policy
- Teaching online safety in school
- Whistleblowing Policy

Appendix 1: Acceptable Use Agreement (staff, governors, volunteers and visitors)

Acceptable use of the school's ICT systems and the internet: agreement for staff, governors, volunteers and visitors	
Name of staff member/governor/volunteer/visitor: **Laptop allocated –** **Equipment must be returned to Business Director**	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device, I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software • Share my password with others or log in to the school's network using someone else's details • Use my personal email, mobile or social media sites to contact students or parents	
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit and my online profiles. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a student informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that students in my care do so too. I will uphold the schools safeguarding policy and online policy	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 2

ICT Acceptable Use Policy - Student

The school has computers with Internet access to aide learning. These rules will help keep you and others safe. You and your parent/carer will have to sign and agree to these before you are allowed to use the ICT facilities.

Using the computers:

- I will only access the computer system with the login and password I have been given and ensure I protect these details.
- I will not access other people's files / computer.
- I will not bring in CDs, Memory Sticks etc. from outside school and use them on the school computers without permission from the Computing teacher.
- I will not change any settings on the school computers without permission
- I will use the equipment for the purpose it is intended.
- I will not move equipment from one computer to another without my teachers permission
- I will not use any device, whether school or personally owned to bully or harass anyone or to send inappropriate content of any type.
- I will not use any websites, apps or services that may bring the school into disrepute
- I understand that any attempt to breach technical safeguards, conceal network identities or gain unauthorised access to any system is unacceptable.

Using the internet:

- Our school filtering system should block all inappropriate material however, I will immediately report to my teacher any unpleasant material that gets through because this will help protect other pupils and myself.
- I understand that the school may check my computer files and may monitor the Internet sites I visit.
- I will not complete and send forms online without permission from my teacher;
- I will not give personal details of any other student when completing forms.
- I will not use any device, whether school or personally owned to access illegal Internet content
- I will not use any device, whether school or personally owned to spread hateful messages or personal views that could cause upset to others.

Using e-mail or other messaging services:

- I will immediately report any unpleasant messages sent to me because this would help protect other pupils and myself.
- I understand that e-mail messages I receive or send may be read by others.
- The messages I send will be polite and responsible.
- I will only e-mail people I know, or my teacher has approved.
- I will not give my full name, my home address or telephone number or that of another student.
- I will not use e-mail or any other form of communications media to arrange to meet anybody other than a Wellacre student outside of school hours.
- I will not send abusive, inappropriate or upsetting messages to anybody via email or any type of communication media

Student Signature:_____ Name (Printed)_____ Date _____

Parent/Carer Signature:_____ Name(Printed)_____ Date _____