GLENWOOD SECONDARY SCHOOL, EMSWORTH

ONLINE SAFETY POLICY

Reviewed	**February 2018**
Responsibility to Review	**HT**
Next Review	**February 2019**
Approval	**GB**
Registered with Information Commissioners Office (date)	**Annual**

This policy should be read in conjunction with other policies including Social Use of Media Policy, Anti-Bullying, Behaviour, PSHE, Data Protection and Freedom of Information policies. This Policy was adapted from the Internet Safety Policy, advice and guidance from attending HCC's Online safety training courses and The Key. Throughout this Policy, reference is made to the Byron Review (June, 2008) which is as relevant today as it was when first published.

➲ https://www.aoc.co.uk/sites/default/files/The_Byron_Review_Action_Plan.pdf

Having considered the evidence, I believe we need to move from a discussion about the media "causing" harm to one which focuses on children and young people, what they bring to technology and how we can use our understanding of how they develop to empower them to manage risks and make the digital world safer. Tanya Byron, 2008

CONTENTS

1. OUR SCHOOL AIM TO:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

1.1 DEFINITION:

Online safety is a **child protection issue not an ICT issue**. All people working at Glenwood School, whether adult or child have a duty to be aware of online safety at all times, to know the required procedures and to act on them in conjunction with the Acceptable Use Agreement. Online safety is not limited to school premises, school equipment or the school day. Neither is it limited to equipment owned by the school. Online safety is a partnership concern i.e. an incident occurring outside school and brought to the school's attention will be treated as if it had happened on school premises in the teaching day. Online safety in the school environment concerns the protection of users, particularly children, of all connectable technology, especially when using the internet, email and mobile communication technology. The Byron Report (2008) provided startling statistics that underline the need for everyone to adopt effective online safety practices and to share the responsibility for child protection.

1.2 STATEMENT OF DUTY OF CARE

"While children are confident with the technology, they are still developing critical evaluation skills and need our help to make wise decisions." (Byron Report 2008)
The Designated Safety Lead staff are the designated online safety officers although all staff have a responsibility to support online safety practices within the school. Children at all levels need to understand their responsibilities and liabilities in the event of deliberate attempts to breach online safety protocols. (See links to other policies).

1.3 SCOPE OF POLICY

Online safety includes the day-to-day running of the physical network and the information passing through it whether connected via the internet or the school's network. Pupils are taught safe practices and that the Online Safety policy will be monitored and enforced. The Online Safety policy links with the Acceptable Use Agreement (KS3, KS4 and staff / visitors). Online safety covers technology not owned by the school i.e. the school responds to online safety threats involving members of its community whether they occurred during the school day, on the school site or if perpetrated using equipment not owned or operated by the school.

2. LEGISLATION AND GUIDANCE

This policy is based on the Department for Education's *Keeping Children Safe in Education*, the statutory safeguarding guidance, 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.
➲ https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

It also 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 pupils' electronic devices where they believe there is a 'good reason' to do so.

3. ROLES AND RESPONISIBILITIES

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation. The governing board will co-ordinate regular 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 as stated in the Acceptable Use Agreement of the school's ICT systems and the internet (Appendix 2)

3.2 The Headteacher

The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school. The Headteacher, as a DSL, is responsible for checking the Securus monitoring server. In this role, the Headteacher is responsible for providing regular reports on online safety to the Governing Body.

3.3 The designated safeguarding lead (DSL)

Details of the school's designated safeguarding leads (DSL) are set out in our child protection and safeguarding policy.

The DSLs take the lead responsibility for online safety in school, in particular:

- Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Headteacher, ICT co-ordinator, and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (Appendix 6) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Liaising with other agencies and/or external services if necessary

This list is not intended to be exhaustive.

3.4 The ICT co-ordinator

The ICT co-ordinator is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
  Currently, this is via the filtered internet connection provided by HCC.
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms, firewall etc. are updated regularly.
  Currently, this is via the filtered internet connection provided by HCC with regular updates etc. installed by Coretek, the school's IT management company.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
  Currently, this is via the filtered internet connection provided by HCC and supported by Coretek, the school's IT management company.
- Ensuring the Securus server which monitors and tracks all equipment and users connected to the network. This flags inappropriate usage against a pre-installed 'dictionary' taking a screenshot of the users screen and detailing the time, PC/laptop used, location of the hardware etc. As online safety is a child protection issue, monitoring the Securus server is undertaken by a Designated Safety Lead member of staff, currently either the Headteacher, Deputy Headteacher or Home-School Link
- Updating and delivering staff training on online safety (Appendix 5 contains a self-audit for staff on online safety training needs)
- Ensure all members of the Glenwood School community, including teaching practise students, Hampshire Futures staff, supply staff and any other visitor who will have access to the School's IT facilities sign an Acceptable Use Agreement (AUA). The AUA is discussed with pupils prior to them signing it. (There is a KS3 and KS4 version of the AUA)
- Ensuring staff have strong passwords i.e. an alphanumeric password, which is subject to six week change by server policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All 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 (appendices 1 and 2), and ensuring that pupils follow the school's terms on acceptable use (appendices 3 & 4)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 6) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the Headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on the Acceptable Use Agreement of the school's ICT systems and internet (appendices 3 & 4)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues?, UK Safer Internet Centre:
  - ➲ *https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues*
- Hot topics, Childnet International:
  - ➲ *http://www.childnet.com/parents-and-carers/hot-topics*
- Parent factsheet, Childnet International:
  - ➲ *http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf*

In addition, the school's website also has a number of useful links for young people and parents, including the very informative Digital Parenting, produced by Vodafone. The school has signed up to receive copies of this magazine which are sent home to parents.

3.7 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 2).

4. STATEMENT OF TEACHING SAFE PRACTICES

"Children and young people need to be empowered to keep themselves safe - this isn't just about a top-down approach. Children will be children - pushing boundaries and taking risks. At a public swimming pool, we have gates, put up signs, have lifeguards and shallow ends, but we also teach children how to swim." Byron Report (2008).

Pupils entering Glenwood School, like young people anywhere, are increasingly familiar with mobile technology but often lack the corresponding level of awareness of online safety. It is therefore essential that during their time here they develop an understanding of how to enjoy mobile technologies but at the same time learn how to reduce their vulnerability e.g. by either doing something of their own volition (or through coercion) or unwittingly making information available that unscrupulous people will benefit from etc. Teaching safe practices applies to staff and governors as well as pupils. Whilst online safety is emphasised to pupils on a daily basis, discrete online safety awareness lessons are provided across the whole school with age-appropriate activities during the spring term to coincide with Safer Internet Day.

4.1 EDUCATING PUPILS ABOUT ONLINE SAFETY

Pupils will be taught about online safety as part of the curriculum in line with the National Curriculum.

In **Key Stage 3**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

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 pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

5. SUPPORTING AND EDUCATING PARENTS ABOUT ONLINE SAFETY

"There is a generational digital divide which means that parents do not necessarily feel equipped to help their children in this space - which can lead to fear and a sense of helplessness. This can be compounded by a risk-averse culture where we are inclined to keep our children 'indoors' despite their developmental needs to socialise and take risks." (Bryon Report, 2008)

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents. Online safety will also be covered during parents' evenings and EHCP reviews.

The school's website has a range of links to websites that support parents and young people in developing safe use of the online world. In addition, Glenwood School is registered to receive copies of Vodafone's 'Digital Parenting' magazine for distribution to parents and copies of the School's Acceptable Use Agreement are also sent home to facilitate discussion. In addition, parents are informed of the online safety procedures and systems used in school. Furthermore, the following is given to parents:

Using the internet is great for young people's education and development. It opens up exciting new opportunities for learning. Whatever they're up to – researching a school project, chatting with friends or playing a game – your children are likely to spend even more time surfing the web as they get older. Fortunately, there are some simple things you can do to help them surf safely and feel confident about learning online. An area on the school website (Online Safety) is provided to offer advice on online safety and links to useful websites.

Parents are also advised:

- that wireless networks should be properly encrypted.
- that an unencrypted network may allow others to see and access computers and peripheral devices connected to it.
- that computers should be in a public area.
- that it is good practice where there is a case for the computer being in a bedroom or other out of line of sight location for an agreement to be reached stating that the computer will be monitored from time to time.
- that robust all round anti-virus/spyware/malware solutions should be in place at all times and updated frequently in line with the manufacturer's guidance.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the Headteacher.

NB: The school will not recommend or offer support to parents regarding hardware or software.

6. CYBER-BULLYING

6.1 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. (See also the school's Behaviour Policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school actively discusses cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. There are dedicated online safety lessons to coincide with Safer Internet Day delivered by the ICT co-ordinator, form tutors discuss cyber-bullying with their tutor groups, and the issue is addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 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 pupils' 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, and/or
- Disrupt teaching, and/or
- Break any of the school rules

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 senior leadership team to decide whether they should:

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

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

➲ *https://www.gov.uk/government/publications/searching-screening-and-confiscation*

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

7. ACCEPTABLE USE OF THE INTERNET IN SCHOOL

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant. (appendices 1 - 4).

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 pupils, 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.

8. PUPILS USING MOBILE DEVICES IN SCHOOL

Pupils may bring mobile devices into school, but are not permitted to use them during:

- Lessons
- Tutor group time
- Clubs before or after school, or any other activities organised by the school

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendix 1).

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

9. PROCEDURES TO BE FOLLOWED IN THE EVENT OF A BREACH OF ONLINE SAFETY / MISUSE

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

- all concerns related to online safety, whether by direct observation or disclosure will be taken seriously.
- staff complete the Online Safety Incident Report form and pass onto a DSL, currently the Headteacher, Deputy Headteacher and Home-School Link.
- the online safety reporting procedure may result, in the opinion of a DSL, escalation including liaising with others e.g. HCC, Police, parents etc.
- Online safety breaches are linked with other policies i.e. Child Protection, Acceptable Use & disciplinary policies. *(Online safety incident recording sheet attached)*

10. STAFF USING MOBILE DEVICES OUT OF SCHOOL e.g. Laptops

Prior to allocation, staff sign to use the laptops in an agreed way – what they are and are not to be used for and will be subject to monitoring. There is a clear expectation that teacher laptops, (and all school-provided equipment) will only be used by the employee of the school i.e. not family members, friends, etc.

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.

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

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

10.1 DATA TRANSFER OFFSITE

There are strict guidelines regarding taking data off the premises and the following need points require consideration before permission is given to use data offsite.

- The purpose
- What the data is e.g. is it a list of first names or a full SIMS list of personal information
- By whom
- When
- How

Where data of a personal nature such as school reports, IEPs, photographs, assessment data etc. is taken home on a school laptop or other storage device, it must be recognised that this data comes under the Data Protection Act and is subject to the school's Data Protection Policy. Care must be taken to ensure its integrity and security. It must not be transferred to home computers and should be removed from any portable device including USB pens and memory cards as soon as is practical. Where staff are using their own digital equipment e.g. cameras and mobile phones, extreme caution is advised to avoid misinterpretation by others. Files should be transferred to school equipment as soon as possible.

The facility exists to allow staff to 'remote-in' to the school network from their school provided laptop; in effect, this provides the same level of security as if staff were working on the school premises.

10.2 STAFF BRINGING IN FILES FROM HOME FOR TEACHING AND LEARNING

Staff must be clear that it is expected that they will check that the file they propose to use in school is free from virus/spyware/malware. The DVD, USB stick etc. must then be scanned prior to use on a school PC / laptop. Files emailed using the Office 365 email facility, provided by Hampshire County Council, are automatically scanned. Staff are clear that it is their responsibility to ensure that the material contained in the file is fit for purpose and does not contain any offensive or copyright material.

10.3 SOCIAL NETWORKING

Staff must **NOT** correspond with pupils using their own personal social messaging site
Staff must **NOT** use any image related to school on any social networking site
Staff must **NOT** discuss school related matters on any social networking site
Pupils attempting to make staff a 'friend' or **any** concerns staff have **must** be reported to the Headteacher.

11. 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.
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, e-bulletins and staff meetings).

The DSLs 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.

Volunteers will receive appropriate training and updates, if applicable.

12. MONITORING ARRANGEMENTS

This policy will be reviewed annually by the ICT co-ordinator. 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:

- Child protection and safeguarding policy
- Behaviour policy
- Social use of media policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure

Appendix 1a

GLENWOOD SCHOOL: (Adapted from 360° Safe AUP Guidelines)

Acceptable Usage Agreement (KS 3 pupils and parents/carers) 2017-18

These rules have been written to make sure that you stay safe when using the computers. When you sign you have agreed to follow these rules. We will talk about these rules before you sign them and a copy will be sent home to your parents.

☺ I will be careful when going on the internet.

☺ I will only use the internet when a member of staff is with me.

☺ I will tell a member of staff if I see something that upsets me.

☺ I know people online might not be who they say they are i.e. A STRANGER

☺ I will be polite when talking to people or writing online.

☺ I will be careful when using equipment.

☺ I will keep my password secret, but I can tell staff if necessary

☺ I will keep my workstation tidy and log off properly.

☹ I will never tell anyone any personal details such as my phone number, address without checking with my parents or member of staff first

☹ I will never arrange to meet someone without telling my parents first

☹ I will never logon using someone else's username.

☹ I will never put water bottles etc. near a workstation

☹ I will never say anything that others might think is unkind.

If I bring a personal mobile phone or other personal electronic device into school:

- I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a member of staff's permission
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

Print name: **Signed (pupil):**	**Date:**
Supported by member of staff (if applicable): **Print name:**	**Date:**

Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Print name: **Signed (parent/carer):**	**Date:**

Appendix 1b

GLENWOOD SCHOOL: (Adapted from 360^{o} Safe AUP Guidelines)

Acceptable Usage Agreement (KS 4 pupils and parents/carers) 2017-18

By using the ICT facilities in school, you have agreed to follow these rules. These rules will be discussed with you as a class before you sign them. A copy of this will also be sent home to your parents.

If you have any questions, please ask a member of staff.

- I will only use the ICT facilities when a member of staff is present.
- I will not logon to another person's account
- I will think before deleting files
- I will treat the equipment carefully
- I will keep my password secure, but I understand I can share it with a member of staff
- I will not install any software or hardware (including memory sticks) without permission from a member of staff
- I will not deliberately access any inappropriate websites
- When communicating online e.g. a smartphone I will think about the words that I use and will not use words that may offend other people
- When communicating online, I will not give my personal information to anyone without the permission of my parent/carer or teacher such as my name, school, email address or phone no.
- I understand that people online might not be who they say they are – some people lie
- I know that the staff can, and will, check the files and websites I have used
- I will not open any attachments in emails, or follow any links in emails, without first checking with a teacher
- I will not arrange to meet anyone offline without first telling my parent/carer, or without adult supervision
- I understand that if I am acting inappropriately then my access to the facilities may be withdrawn and my parents/carers may also be informed.

If I bring a personal mobile phone or other personal electronic device into school:

- I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a member of staff's permission
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

Print name: **Signed (pupil):**	**Date:**
Supported by member of staff (if applicable): **Print name:**	**Date:**

Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Print name: **Signed (parent/carer):**	**Date:**

GLENWOOD SCHOOL: (Adapted from 360° Safe AUP Guidelines)

Acceptable Usage Agreement (Governors, volunteers and visitors) 2017-18

Name of Governor/volunteer/visitor: ___________________________________

Name of agency / company if applicable: ___________________________________

You have been asked to sign this form as you may have access to the school's ICT facilities during your visit to Glenwood School. This may be a one-off visit or you may be a regular visitor. Please read and sign this form and return it to Reception. It will remain valid for the academic year 2017 – 2018.

These guidelines set out the basic principles for how visitors to Glenwood School use ICT, including the Internet and guidance about the use of social networking sites out of school. These principles can be summarised as: ensuring pupils remain safe, ensuring all adults remain safe and ensure all adults always 'model' good practise. If you have any questions regarding these guidelines, please see a member of the Senior Management Team. By signing this you agree to the school having the right to examine any content – emails, files, photos etc. and monitor your internet use.

If you suspect there is an e-safety issue i.e. a Child Protection issue please see the Headteacher, Deputy Headteacher or Home-School Liaison Officer as soon as possible. Report any technical issues to the ICT Co-ordinator.

Use of ICT resources

Use computers and equipment with care and ensure pupils do the same
Return cameras and microphones etc. after use (remove pictures/files as data may be deleted)
Store all photographs in 'Photos' – (Photos in Curriculum will be deleted)
Try not to be wasteful, e.g. batteries, printer ink (use draft) and paper (print both sides)
Scan all removable storage– memory sticks etc. for viruses prior to use
Do not install any software
Understand that inappropriate use of the school's network may result in some services being removed and further action being taken by the Headteacher

Online Behaviour / Safe Working Practises

Do not share your password with pupils or other staff (except the ICT technician / ICT Co-ordinator)
NEVER allow pupils to use your account
Log off when you have finished using a computer or leave the computer unattended
Ensure your online activity is related to professional duties only
Do not use the school's ICT resources for financial gain e.g. auction or betting sites or to access inappropriate sites e.g. racist or pornographic sites etc.
Online dialogue e.g. emails with schools, parents or organisations etc. must remain professional at all times.

Data Protection

School data must not be removed from the premises.
You must not use your personal camera / phone to take school related images.

Social Networking

You must **NOT** correspond with pupils using any social networking site
You must **NOT** use any image related to Glenwood School on any social networking site
You must **NOT** discuss school related matters on any social networking site
Please report any concerns you may have e.g. pupils attempting to make you a 'friend' or any other concern you may have to the Headteacher even if you are no longer associated with Glenwood School.

Signed (governor/volunteer/visitor):	**Date:**

GLENWOOD SCHOOL: (Adapted from 360° Safe AUP Guidelines)

Acceptable Usage Agreement (Staff) 2017-18

Name: __________________________________

These guidelines set out the basic principles for how staff use ICT, including the Internet, at Glenwood School and also their use of social networking sites out of school. These principles can be summarised as: ensuring pupils remain safe, ensuring staff remain safe and ensure staff always 'model' good practise. If staff have any questions or concerns regarding these guidelines, they should direct them to a Designated Safeguarding Lead (safeguarding issues) or the ICT Coordinator (technical issues). By signing this you agree to the school having the right to examine any content – emails, files, photos etc. and track your internet use.

Use of ICT resources

Use computers and equipment with care and ensure pupils do the same
Return cameras and microphones etc. after use (remove pictures/files as data may be deleted)
Store all photographs in the Photo Gallery drive
NB: Photos in your personal account or the Curriculum drive will be deleted
Use resources economically; purchase rechargeable batteries, print in draft and print on both sides of paper
Scan all removable storage– memory sticks etc. for viruses prior to use
Do not install software not authorised by the ICT co-ordinator / ICT technician
Understand that inappropriate use of the school's network may result in some services being removed and further action being taken by the Headteacher
Return any hardware or equipment if you are no longer employed by the school

Online Behaviour / Safe Working Practises

Do not share your password with pupils or other staff. If you forget your password it can be easily reset.
Use a strong password (upper and lower case letters and symbols e.g. $, £ etc.) and change it when required
DO NOT permit pupils to use your account.
Log off when you have finished using a computer or leave the computer unattended
Online activity is related to professional duty (although personal use is permitted within reason and does not occur within 'directed time' i.e. lessons etc.
Do not use the school's ICT resources for financial gain e.g. auction or betting sites or to access inappropriate sites e.g. racist or pornographic sites etc.
Online dialogue e.g. emails with schools, parents or organisations etc. must remain professional at all times.

Data Protection

Where data of a personal nature such as school reports, IEPs, photographs, assessment data etc. is taken home on a school laptop or other storage device, it must be recognised that this data comes under the Data Protection Act and is subject to the school's Data Protection Policy. Care must be taken to ensure its integrity and security. It must not be transferred to home computers and should be removed from any portable device including USB pens and memory cards as soon as is practical.
Where staff are using their own digital equipment e.g. cameras and mobile phones, extreme caution is advised to avoid misinterpretation by others. Files should be transferred to school equipment as soon as possible;

Social Networking

You must **NOT** correspond with pupils using your own personal social messaging site
You must **NOT** use any image related to school on any social networking site
You must **NOT** discuss school related matters on any social networking site
Pupils attempting to make you a 'friend' or **any** concerns you have **must** be reported to the Headteacher

You will be required to complete a new form at the start of each academic year.

Signed: **Date:**

Appendix 4

GLENWOOD SCHOOL:

Staff online safety training needs audit (2017-18)

Name of staff member: ________________________________	**Date: _____________**
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training? Please record them here.	

Glenwood School **Online Safety Incident Record** **Please complete as fully as possible and give to Designated Safeguarding Lead** **APPENDIX 5**

Date:	Time:	Location:		
Name of member of staff discovering incident		Name of pupils(s) (or if an adult) involved in the incident:		
Nature of incident *Tick ✓*	Intentional access to inappropriate material	Cyber bullying	Grooming	Other
Details				
The event occurred	During a lesson	During breaks etc.	Outside school hours (inc. home)	

Headteacher / Deputy Head / CPO actions

If a member of staff	HCC Personnel Dept. contacted	Recommended action	Action applied	Chair of Governors involvement
If ‘other’ e.g. contractor				
If a pupil	Parents contacted	Date	Time	Attach notes of conversation
	Parents / carers Interviewed	Date	Time	Attach notes of meeting
	Action			
Attached	Screenshots:	Statement from:	Telephone conversations with:	Interview minutes with:
	Other:			