# Online Safety Policy (A8)

| | |
|---|---|
| Scope: | Whole School (Including Boarding) |
| Release date: | September 2023 |
| Author: | Senior Deputy Head Senior School |
| Reviewer: | Deputy Head Academic |
| Approval body: | Board of Directors<br>*(released pending ratification at Michaelmas Term Board Meeting)* |
| Review date: | May 2024 |

**Linked documents**

This Policy should be read in conjunction with the:

- The Safeguarding and Child Protection Policy (A1)
- Child-on-Child Abuse Policy (A8)
- Behaviour Policy (A4)
- 10.4 of the Parent/School Contract - this refers to permitted uses of imagery and photographs

**Availability**

This Policy is available to parents and prospective parents on the School website, and a printed copy may be requested from the School Offices/Pupil Services Team.

**Edition Changes**

| **Edition Release 2023**<br>**Location of change** | **Clause impacted** |
|---|---|
| **Throughout document:**<br>• Magdalene House changed to Prep School<br>• Peer on Peer changed to Child on Child | |

## Contents

## Purpose

This document sets out the approach that Wisbech Grammar School, comprising the Senior School and Prep School, takes to online safety. It provides a strategic framework to maximise the educational uses of IT and to minimise online safety risks, both to individuals and to the reputation of the School.

## Policy Statement

Wisbech Grammar School embraces the use of technology, including the internet (social media), and recognises it as an essential tool for education, business, and social interaction. It enables a richer learning environment to be provided for our pupils, and its use is a key life skill.

The School also recognises that the use of technology poses potential risks to pupils and staff and that it has a responsibility to minimise those risks when they are in school and to help them understand and manage them in their lives beyond school.

The School follows national guidance in defining online safety as relating to:

"…all fixed and mobile technologies that children may encounter, now and in the future, which allow them access to content and communications that could raise issues or pose risks to their wellbeing and safety".

Online Safety risks can never be completely eliminated, but the School takes every step it can to minimise them and has robust procedures in place to deal with any incidents that do occur and then to learn from them.

In determining risks to be addressed the School follows the framework set out in the Byron Review report 'Safer Children in a Digital World'. It recognises that many of those risks could apply to its staff as well as its pupils.

The School's approach, based on national guidance, is to minimise the risks for everyone in its community through an appropriate combination of:

- Policies and procedures,
- Technical safeguards,
- Education and training.

Those strands are under-pinned by regular monitoring and review to ensure that expected standards are being achieved. Reviews also consider whether the approach needs to be revised to take account of new technology or changing trends in behaviour. For example, does an upsurge in 'sexting' amongst young people nationally require any changes to the curriculum?

## Policies and Procedures

To implement its overall approach to online safety, Wisbech Grammar School has the following more detailed policies and procedures in place:

**Policies**

**1. Online Safety Roles and Responsibilities (Appendix A)**

Every member of the Wisbech Grammar School community has a shared responsibility for online safety. This policy sets out the expectations on different groups within the school community. It is included as Appendix A of this document and is reviewed annually. Overall Responsibility for Online Safety lies with the Designated Safeguarding Lead who works with the Assistant Head Academic Administration.

**2. Acceptable Use Policy for All Staff (Appendix B)**

This sets out the detailed framework to guide staff in what is and what is not regarded as acceptable use of technology. It is reviewed annually and staff are required to sign that they have read and understood it after any significant changes.

**3. EYFS Policy for the use of Cameras and Mobile Phones (Appendix C)**

This sets out what is expected with regard to the use of the above devices by those specifically working in the EYFS areas of the school community.

**4. Acceptable Use Policy for Pupils (Appendix D)**

This sets outs the expected level of behaviour from pupils when using technology. It is reviewed annually and all pupils are required to sign to say that they have read and understood it. Parents are asked to counter-sign the agreement to show that they are aware of the School's policy.

**5. Acceptable Use Policy for Visitors (Appendix E)**

This sets out the expectation on guests when using either their own or the School's technology on school premises. It is displayed prominently at the school reception and next to relevant computer equipment. It is reviewed annually.

## 6. The Safeguarding and Child Protection Policy and other related Policies

Online Safety is not primarily a technology issue but a safeguarding issue. This online safety Policy should be read in conjunction with the School's wider Safeguarding and Child Protection Policy, Child-on-Child Policy and Behaviour Policy, all of which can be found on the School website. It is part of the ethos of Wisbech Grammar School to promote considerate behaviour and to value diversity. Abuse and harassment in any form should always be reported to a member of staff. It is never the victim's fault and they should not be afraid to come forward.

Cyber bullying is a particularly damaging form of Child-on-Child abuse, because it can be so pervasive and anonymous. There can be no safe haven for the victim, who can be targeted at any time or place. The School's Child-on-Child Abuse policy describes the preventative measures and the procedures which will be followed when cases of Abuse are discovered. All members of the school community should be aware that social networking sites can provide a platform for constructive activity but they should also be aware that such sites can provide an ideal environment for Abuse. Social networking sites are barred from the school network unless deemed appropriate for educational purposes by a member of staff. Parents are advised that if they allow their children to access social networking sites then their use should be carefully monitored. If using such sites at home pupils are advised that they should consider their posts with the utmost care. Not befriend people they don't know in the real world and recognise that people may be pretending to be someone else to orchestrate abuse either online or offline. Staff should not accept pupils as friends on these sites.

### Procedures

Wisbech Grammar School has various procedures in place to ensure that all members of the community know what to do when there are issues with an online Safety dimension

a. **Online Safety incidents**
   The procedure for dealing with an online safety incident is set out in Appendix F.
b. **Internet filtering**
   Requests for changes to the Internet filtering are set out in Appendix G.
c. **IT system changes**
   Any other IT system changes must be sanctioned by the IT Support team and may require discussion with senior management and/or the Board of Directors.
d. **Personal devices**
   Personal devices may only be connected to the BYOD (Bring Your Own Device) network unless specifically approved otherwise. Personal devices found on the School's private network, especially in those areas concerned with sensitive information, will be removed and the incident reported to an appropriate Designated Person. Boarders will also use the BYOD network for their personal devices
e. **Staff guidelines for taking pupils photographs**
   The procedure for this is set out in Appendix H.
f. **Staff guidelines for the potential risk of radicalisation for pupils using social media**
   The procedure for this is set out in Appendix I.
g. **Guidelines for visitors**
   Visitors will be asked to sign Appendix E: The Visitors' Acceptable Use Policy when they arrive at school. It will be sent out in advance for those pupils scheduled to attend taster days. Signed copies will be collected before or on the day they arrive.

## Technical Safeguards

Wisbech Grammar School's technical safeguards are under constant review. Currently the School maintains the following systems as part of its online safety strategy:

### 1. Internet Filtering

All access to the internet from within school goes through a filtering system which blocks access to all illegal and the majority of inappropriate content. All requests for changes to the filtering are made by staff to the IT Support Department following the procedure described in Appendix G. Pupils are encouraged to report to staff any content they are able to access that makes them feel uncomfortable.

### 2. Internet and Network Usage Monitoring

Wisbech Grammar School reserves the right to monitor routinely all the School's electronic systems and their use by pupils, staff, Advisory Committee Members, Directors and visitors.

All files which are opened on the School's network are routinely scanned by monitoring software. This software searches for certain key terms and flags their use. Words of a sexual nature and swear words are flagged immediately. The user name, time of use and workstation are recorded. A screenshot is taken of the page flagged. The IT Support Department will then refer this to the appropriate senior member of staff. The Headmaster (or his nominated senior member of staff) reserves the right to review any data that is found on the school network or a school machine.

### 3. Anti-virus

The School uses anti-virus software. All members of the school community are made aware of the dangers caused by computer viruses. If there is any suspicion that hardware, a file or storage device has a virus or will spread a virus it should be taken to the IT Support Department who will take appropriate action.

### 4. Email Filtering

In addition to viruses the Wisbech Grammar School email system will be filtered for spam messages. It is not possible to eradicate spam entirely but every effort is made to reduce it to a minimum.

## 5. Education and Training

Whilst not under-estimating the value of policies and technical safeguards, it is Wisbech Grammar School's view that education is the most important weapon in its armoury for keeping staff and pupils safe. Whilst policies and technical safeguards may help protect children during their school career and while they are on the premises, education can give them the skills to keep themselves and others safe wherever they are.

## 6. Staff, Advisory Committee Members and Directors

All new staff and Advisory Committee Members and Directors are provided with information about the school's online safety policies and procedures as part of their induction. All staff receive training in online safety issues. This includes an understanding of what OFSTED and ISI inspectors expect of a school workforce. The School's annual CPD planning process includes identifying the need for any additional online safety training related to particular roles, responsibilities or newly identified issues. All staff are also given training on the School's filtering and monitoring systems at induction, in line with KCSIE 2023.

## 7. Pupils

The School's comprehensive PSHCE programme on online safety is the responsibility of the PSHCE Co-ordinator, who liaises with the Designated Safeguarding Lead and Heads of Section. All year groups in the school are educated in the risks and the reasons why they need to behave responsibly online.

## 8. Parents and Guardians

The School seeks to work closely with parents and guardians in promoting a culture of online safety. The School will contact parents if there are any concerns about behaviour in this area, and encourage parents to discuss their concerns with the School. The School recognises that not all parents and guardians may feel knowledgeable to protect their child when they use IT at home; therefore discussion afternoon/evening are arranged for parents when appropriate. The School will also endeavour to help parents understand these issues, using appropriate media.

## 9. Sanctions

Failure to comply with the Acceptable Use Policy for Pupils may result in loss of access to the School network/ internet, detentions, suspensions, exclusions, contact with parents and, in the event of suspected illegal activities, involvement of the police. Pupils' personal devices may also be confiscated.

Failure to comply with the Acceptable Use Policy for Staff, whether in or out of school, may result in disciplinary action. This may include loss of access to the School network, invocation of the School's disciplinary process (up to and including a Board of Directors' Disciplinary Panel), dismissal or, in the event of illegal activities, involvement of the police.

## Appendix A: Online Safety Roles and Responsibilities

Safeguarding is a shared responsibility and can only be effective if every member of the Wisbech Grammar School community is aware of the responsibilities appropriate to their respective roles.

The Board of Directors are responsible for:

- Approval of the online safety and related policies and for reviewing their effectiveness,
- Receiving regular information about online safety incidents through the nominated Advisory Committee Member for Safeguarding and Child Protection.

The Headmaster is responsible for:

- Ensuring the safety (including online safety) of the school community, although day to day responsibility for online safety is delegated to the Head of Digital Literacy,
- Ensuring that the The Designated Safeguarding Lead and other relevant staff receive suitable CPD to enable them to carry out their online safety roles,
- Ensuring that there is a system in place to allow for monitoring and support of those in school who carry out the e-Safeguarding role.

Designated Safeguarding Lead is responsible for:

- Day to day online safety issues,
- Ensuring all staff are aware of the school's systems and procedures for Filtering and Monitoring,
- Ensuring that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place,
- Ensuring that staff are trained and advised on online safety issues,
- Liaising with school IT technical staff,
- Receiving reports on online safety incidents and ensuring that they are logged by staff using the standard 'Logging Concern' sheets for safeguarding, where appropriate,
- Meeting regularly with the nominated Advisory Committee for Child Protection to discuss current issues,
- Meeting regularly with the nominated Safeguarding Director to discuss current issues,
- Reporting regularly to the Headmaster/Senior Team.

The IT Support Staff are responsible for:

- Ensuring the school's IT infrastructure is secure and is not open to misuse or malicious attack,
- Ensuring the School meets the online safety technical requirements for this policy to operate,
- Enforcing password protection policies to ensure school system passwords are secured and regularly changed,
- Keeping up to date with online safety technical information and advising the The Designated Safeguarding Lead of implications for the School's policies or procedures,
- Monitoring for the misuse or attempted misuse of the network or remote access, email and reporting this to the Designated Safeguarding Lead using the appropriate documentation,
- Implementing and updating filtering and monitoring software.

Teaching and Support Staff are responsible for:

- Maintaining up to date awareness of online safety matters and of the current School Online Safety policies and procedures, including those related to the use of mobile phones, cameras and handheld devices (refer to Appendix I),
- Reading, understanding, and signing the School's Acceptable Use Policy for Staff (AUP),
- Reporting any suspected misuse or problem through the normal Safeguarding and Child Protection routes or, where appropriate, to the IT Support Department,
- Ensuring their digital communications with pupils (including email) are on a professional level and only carried out using official school accounts and systems,
- Ensuring online safety is considered as part of the planning of the curriculum or other school activities where relevant,
- Helping pupils to understand and follow the School online safety rules and AUP,
- Helping pupils have a good understanding of research skills and the need to avoid plagiarism and judge content that is biased or not relevant,
- Monitoring IT activity in lessons, extra-curricular and extended school activities,
- Ensuring in lessons where internet use is pre-planned, that pupils are guided to sites checked as accessible through the school systems and suitable for their use, and that they report any unsuitable material that is found,
- Ensuring their personal behaviour does not put them, their pupils, the School or their professional reputation at risk.

Pupils are responsible for:

- Doing everything they can to keep themselves safe,
- Doing everything they can to keep others safe.

Parents/Carers are responsible for:

- Endorsing (by signature) the Acceptable Use Policy for Pupils,
- Alerting the School to any concerns they may have about their own child or any other member of the school community.

# Appendix B: Acceptable Use Policy for Staff

### Key Principles

I understand that I have a personal responsibility for helping to ensure that all members of the school community are kept as safe as possible when using technology and that my own behaviour should set an example.

I will not do anything that could lead to the School suffering a loss of reputation.

I will ensure that I am sufficiently aware of the issues around online safety, including cyber bullying, to be able to make a judgement about whether any activity I am planning or participating in involves any risks. If I feel I need further training or advice I will raise this with a senior member of staff.

If I identify any risks that I cannot manage myself, I will consult my Head of Section.

If I become aware of any incident involving technology I will report it using the normal safeguarding procedures, as set out in the School's Safeguarding and Child Protection Policy. (see Wisbech Grammar School website).

I understand that the School IT systems are primarily intended for educational use. I will limit my personal use to appropriate times and purposes. I will not use either the School's or my own technology in ways that put the School's systems at risk, prevent other users from legitimately making use of them, or bring the School into disrepute.

I understand that if I fail to comply with the School's policies and procedures, or in any other way put members of the school community at risk through the use of technology, I may face disciplinary action including the possibility of dismissal. Suspicion of illegal activity may result in me being reported to the police.

### Guide to Acceptable Behaviours

Technology changes rapidly and it is not possible to document every use or expected behaviour. For that reason it is essential that staff are able to apply the principles of the School's Online Safety policy to new situations.

Within the key principles set out above, as a minimum, the School expects the following commitments:

**Content**

I will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programs or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.

I will ensure that I check any online materials or websites that I intend to use with pupils in advance of the lesson to ensure that they are appropriate and accessible from School systems.

I will immediately report any unpleasant or inappropriate material or messages, anything that makes me feel uncomfortable when I see it on-line, or anything that I believe poses a risk to a member of the school community.

I will ensure that I have permission to use the original work of others in my own work and indicate the original source. I understand that plagiarism is unacceptable and if discovered it will have serious consequences. I will take every appropriate opportunity to ensure that pupils understand this.

Where work is protected by copyright, I will not try to download copies (including music and videos) unless I have the permission of the copyright owner, either directly or within the terms of a school licence.

**Communication**

I will be polite and responsible when I communicate with others.

I will only transact school business on the school's own systems or systems which have been explicitly approved by the Senior Team.

Email is an important part of today's communications systems. Use of the installed systems/connections is for legitimate work related/education purposes only and is encouraged to improve the quality of work, operational matters, education, and development.

I will take care when writing emails or other messages. Due to the sometimes-informal nature of email, texts etc, it is easy to forget that it is a permanent form of written communication and that material can be retrieved even when it is deleted from a computer or other device that has been used. I will think before I send.

I will not open any attachments to emails, unless I know and trust the person/organisation that sent the email, due to the risk of the attachment containing viruses, other harmful programs, or inappropriate content.

If material in an email or other message is thought to be offensive, harmful or defamatory I will alert a Designated Person immediately.

**Personal Use and Professional Reputation**

I understand that technology is made available to me for work duties, work related educational purposes and work related research purposes. My personal use of the internet and other technologies will be limited to lunch breaks and work breaks only. I recognise that personal use is a privilege, not a right and that it may be withdrawn at any time.

I will ensure that I protect my professional reputation and do not do anything online that could jeopardise my professional standing or that of the School.

If I believe that my professional reputation has been put at risk by my own actions or those of others I will inform the appropriate Head of Section, the Senior Deputy Head or the Head of Digital Literacy.

I will not communicate with any pupils except through official systems (such as School email and Teams) and will not become their 'friends' on social networking sites such as Facebook and Instagram.

Please follow these steps when using social media as a digital learning tool:

1. First, I will ensure this tool is appropriate and has a clear educational purpose e.g. it is a tool I have seen promoted in one of the school's Digital Learning Training sessions or during an external INSET course or recommended by another teacher in an article I have read. I will contact the Head of Digital Literacy if I am not sure whether it is appropriate or poses any online safety risks,
2. I will also check there are no age restrictions e.g. pupils should be 13 or older to use social media tools like Twitter or Google Plus,
3. If it is a tool that the School does not currently use, I will check with IT Support that it will work for pupil and staff accounts in school. I accept I may have to wait a reasonable length of time while the tool is set up,
4. I will instruct pupils to use their School email address as part of the registration process and check that they only have to enter limited personal information e.g. name and date of birth. They should not have to enter their address or telephone number,
5. For situations where I would like pupils to access a teacher blog or social media feed, I will first ensure I have changed the settings to the safest level e.g., on Twitter it is possible to set up a feed where new members have to request access or Google Blogger allows teachers to moderate a new post before it can be seen by the online community,
6. Whilst using the tool to share links and facilitate online discussion, I will ensure I remind pupils to follow good digital citizenship advice: ensure messages are polite, sensible and relevant.

Finally, I will ensure I separate personal and educational use of social media tools. E.g., if I already have a personal Twitter account, I will ensure I set up a different one when I use the same tool in the role of teacher. The same goes for Facebook. I will never accept or send friend requests from present pupils other than immediate family (in this case I will inform the Designated Safeguarding Lead).

Likewise, if I want to use social media with my pupils for educational use, I will need to set up a new teacher account first. I will never post personal photos or messages to this online space.

I will not accept past pupils as friends on social media who were at school the previous year and I understand that it is a recommendation that I should not accept past pupils who have left in the

last five years.

I will not use the School IT systems for on-line gaming or on-line gambling, nor use my own technology for those purposes whilst on school premises or when on school business.

I will only use my personal hand held/external devices (mobile phones/USB devices etc) in school if appropriate; I understand that, if I do use my own devices in school, I should follow the rules set out in this agreement, in the same way as if I was using school equipment.

I understand that, for my own protection and that of others; the School may monitor and record my use of its IT systems. I understand that the School will do everything it can to support me if I am the victim of any online safety related incidents.

**Data Protection**

I will not share my username and password, print it or store it online. Nor will I use any other person's username or password.

I will ensure that I do not leave a computer logged on after use or leave a computer logged on unattended.

I will not take or distribute images of anyone without their permission or, in the case of pupils, that of their parents.

I will not upload or send any personal information about staff or pupils unless I am satisfied that I am meeting the requirements of the Data Protection Act.

**Security and Health & Safety**

I recognise that the security of software programs and data is most important. I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.

I will immediately report any damage or faults involving equipment or software, however this may have happened.

I will ensure that all files/disks/storage devices are virus checked by the IT Support Department. If I suspect that a virus is present on any piece of equipment I will report it immediately to the IT Support Department.

I will not install or attempt to install programs of any type on a machine, or store programs on a computer, nor will I try to alter computer settings. All software must be authorised by the IT Support Manager.

I will not use any network account other than the one that has been assigned to me, nor try to access areas of the computer network other than my own.

At all times I will take care to comply with HSE guidelines on the use of VDUs, keyboards and work stations.

I will take every reasonable measure to ensure that school equipment is not lost, stolen or damaged. I will never leave the School's mobile devices, such as laptops, unattended.

I understand that losses incurred by the School as a result of wilful, careless or irresponsible behaviour may lead to the costs being passed on to me.

**Dealing with incidents**

I understand that any serious concerns I have should be shared immediately with a Designated Person.

In the event that I come across any inappropriate material (such as pornography) or illegal content (such as child pornography) on any device, I will also:

- Leave the equipment in question alone and contact the IT Support Department immediately,
- Under no circumstances will I continue using the equipment, though I may cover up the screen to avoid further inadvertent viewing of the material,
- I will not copy, print, send or unnecessarily show the material to any other member of staff,
- I will leave the equipment's vicinity and wait until a member of the IT Support Department arrives,
- I will discourage anyone else from using the equipment and note any use of the computer equipment by others and report it to the member of the IT Support Department on his/her arrival,
- If I find the experience distressing I understand that I will be offered support through confidential counselling.

WISBECH GRAMMAR SCHOOL

## Acceptable Use Policy for Staff:  Staff Agreement

Name……

Department: ……

I have read and understand Wisbech Grammar School's Online Safety and related policies, including the Staff Acceptable Use Policy attached.

I understand that failure to follow these policies may result in disciplinary action being taken, including the possibility of dismissal.

Signed: …….

Date: ……..

Print name: ……

## Appendix C: EYFS Policy for the use of cameras & mobile phones/devices

To ensure the safety and welfare of the children in our care this policy outlines the protocols for the use of personal mobile phones/devices and cameras in the EYFS setting at Wisbech Grammar School.

- Personal mobile phones, cameras and video recording equipment cannot be used when in the presence of children on school premises including the swimming pool,
- All mobile phones must be stored in the Staff room. during contact time with children. (This includes staff, visitors, parents, volunteers and students),
- No parent is permitted to use their mobile phone or use its camera facility whilst inside school buildings, in the swimming pool or around the grounds when children are present,
- Mobile phones must not be used in any teaching area within the setting or within the bathroom area,
- In the case of a personal emergency staff should use the school telephone. It is the responsibility of all staff to make families aware of the school telephone numbers,
- Personal calls may be made in non-contact time but not within the teaching areas,
- Personal mobiles, cameras or video recorders should not be used to record classroom activities. School equipment only should be used and parental consent is sought in advance of photos being taken,
- Photographs and recordings can only be transferred to and stored on a school computer/IPad or laptop before printing,
- All telephone contact with Parents/Carers should be made on the school telephone,
- During group outings nominated staff will have access to the school mobile which can be used in an emergency or for contact purposes. Staff may carry their own phones in bags but they should only be used in emergencies.

## Appendix D: Acceptable Use Policy for Pupils in the Senior School

The School's aim is to develop your ability to keep yourself safe when using technology such as the internet, so that you can benefit from it as a learning tool. If there is anything in this document that you do not understand, please ask your Form Tutor.

Please note that the School does not provide charging facilities; all devices must be fully charged when brought into school.

- I will not charge my devices in school,
- I will only use School devices for school purposes,
- I will only use School IT systems (whether accessed from personal or school devices) (including the internet, email, digital video, mobile technologies, etc) for school purposes,
- I will treat School devices with care and respect. If there is any accidental damage I will report it immediately to a teacher,
- I will not download or install software on School devices,
- I will only log on to systems with my own user name and password,
- I will only log on to school iPads with my own AppleID and passcode,
- I will follow the School's IT security system and not reveal my passwords to anyone and change them regularly,
- I will not leave unattended any device on which I have logged on,
- I will only use my School email address,
- I will make sure that all IT communications with pupils, teachers or others are responsible and sensible,
- I will be responsible for my behaviour when using the internet. This includes the resources I access and the language I use,
- I will not attempt to bypass the internet filtering system,
- I understand that all my use of the internet and other related technologies can be monitored and logged and can be made available to my teachers,
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to a teacher,
- Images of pupils and/or staff will only be taken, stored and used for school purposes in line with School policy. They will not be distributed outside the school network without permission,
- I will support the School approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community,
- I will ensure that my online activity, both in and outside school, will not cause the School, the staff, the pupils or anyone else distress, and will not bring the School into disrepute,
- I will not give out any personal information such as my name, phone number or address,
- I will not arrange to meet someone in person whom I have only met online without telling an adult at home or at school,
- I will respect the privacy and ownership of others' work on-line at all times,
- I understand that plagiarism is unacceptable. If discovered, it will have serious consequences, such as the disqualification from public examinations,

- I will take every reasonable step to keep my personal devices and School iPads safe and I will not leave them unattended. Prior to any Sports lessons or activities, I will put any such devices in my locker,
- I understand that these rules are designed to keep me safe and that if they are not followed, School sanctions will be applied and my parent/carer may be contacted.

## Appendix D: Acceptable Use Policy for Pupils in Prep School

- I will only use IT in school for school purposes,
- I will only use my class email address or my own School email address when emailing,
- I will only open email attachments from people I know, or who my teacher has approved,
- I will not tell other people my IT passwords,
- I will only open/delete my own files,
- I will make sure that all IT contact with other children and adults is responsible, polite and sensible,
- I will not deliberately look for, save, or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately,
- I will not give out my own details such as my name, phone number or home address,
- I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me,
- I will be responsible for my behaviour when using IT because I know that these rules are to keep me safe,
- I will support the School approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community,
- I know that my use of IT can be checked and that my parent/carer contacted if a member of Staff is concerned about my online safety.

WISBECH GRAMMAR SCHOOL

## Acceptable Use Policy for Pupils:
## Pupil's Agreement and Parental Confirmation

All pupils use IT systems, including the internet, email, and mobile technologies, in school as an essential part of learning and assessment. Pupils and their parents/carers/guardians are asked to show that they have understood and agree to follow the Acceptable Use Policy.

Before signing this form make sure that you have read the complete document and discussed it with your parent(s)/carer(s)/guardian(s).

Pupil's name: …….. Form: ……..

Pupil's agreement:
I have read and understand the Online Safety and Acceptable Use Policy for Pupils and agree to follow these when:

- I use the School IT systems and equipment (both in and out of school),
- I use my own equipment in school e.g. mobile phones, PDA's, cameras etc,
- I use my own equipment out of school in a way that is related to me being a member of this School e.g. communicating with other members of the School, accessing School email, websites etc.

Signed: ……..…

Date: ……..

WISBECH GRAMMAR SCHOOL

## Parental consent to publish work and photographs:

- I agree that my child's work may be electronically published,
- I also agree that appropriate images and video which include my child may be externally published subject to the school rule that photographs will not be accompanied by pupil names in a manner which would be easy to link individuals to images.

## Parental acceptance of Acceptable Use Policy

- I have read and understood the Acceptable Use Policy for Pupils,
- I understand that my child will be required to use a range of technology, including the internet, to further their learning,
- I understand that the School will take all reasonable steps to ensure the safety of my child while they are using that technology, but accept that there is an element of risk,
- I understand that the School cannot be held responsible for the content of materials accessed through the internet. I agree that the School is not liable for any damages arising from use of the internet facilities or other technology.
-

Signed: …….. Date: …….

Please print name: ……

Relationship to pupil: ……..

*Please return the completed form to your child's Form Tutor or Class Teacher.*

WISBECH GRAMMAR SCHOOL

# Appendix E: Acceptable Use Policy for Visitors

### Visitor Use of School IT Equipment

Visitors who have been given permission by a member of staff to use the School's IT equipment are expected to adhere to the following guidelines:

- I will only use the equipment for the purpose agreed,
- I will immediately report any problem or anything that concerns me to a member of staff,
- I will delete any personal materials, files or data when I finish using the computer,
- I will not attach any personal device to a School computer (including memory sticks and other storage media) unless it has been checked/approved by the IT Support Department,
- I will not use the equipment to access or try to access any material (eg websites) which would be regarded as inappropriate for pupils to see,
- I will not take copies of any files or data that I find on the computer.

### Visitor connection to School network

Visitors who wish to connect their own or the School's IT equipment to the School guest network will be asked to sign a Visitor Declaration and Acceptable Use Policy. The IT Support Department will issue a password for the required period of time.

Visitors are not permitted to connect their own devices to the School's internal network.

Name (please print) _____ Event _____

I understand that I have been given a user name and password to allow me access to the Wisbech Grammar School network

from (time) _____ (date) _____

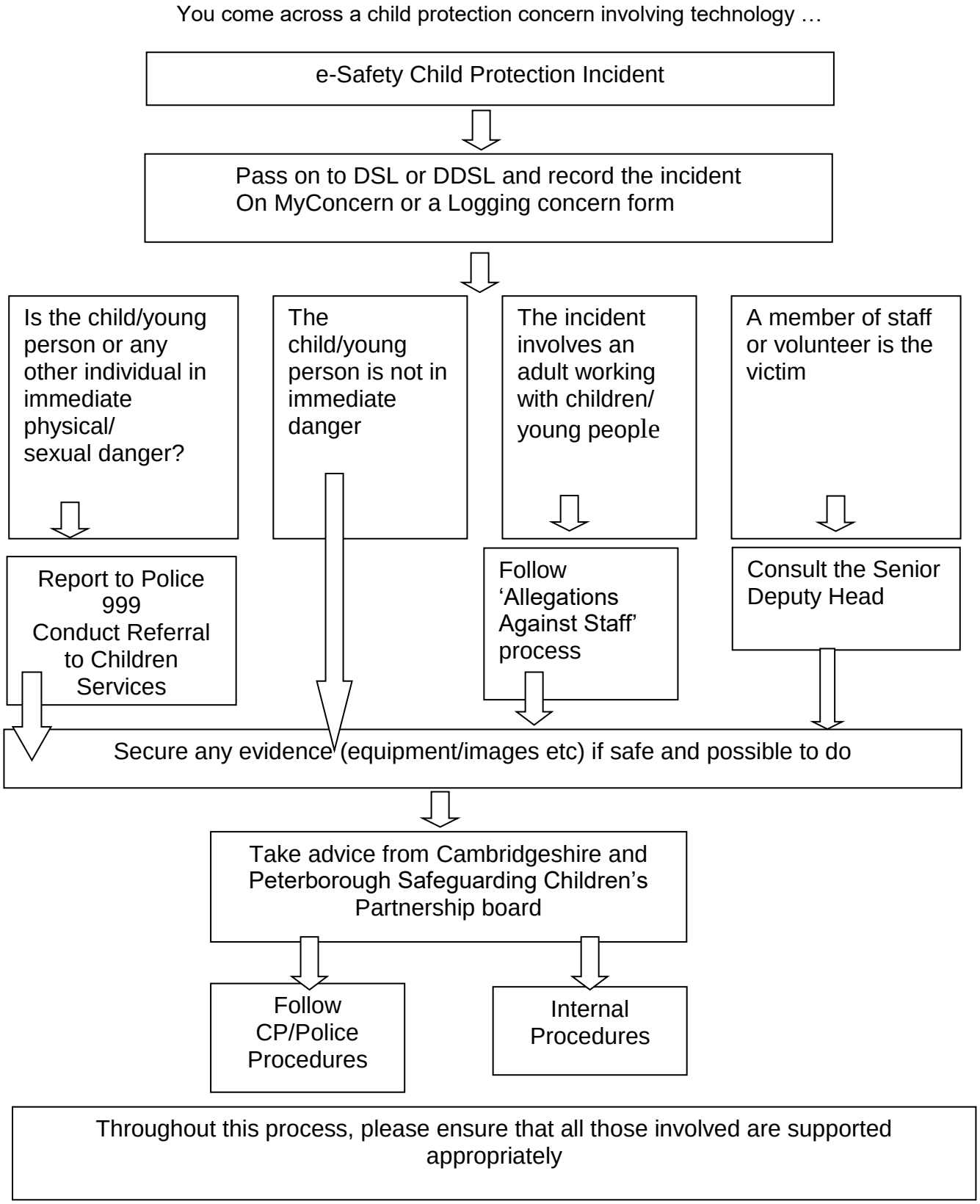
to (time) _____ (date) _____

I understand that the user name and password is for my personal use and I will not share it with anybody else. I will not try to upload, download or access any materials which are illegal or inappropriate in an educational establishment, or which may cause harm or distress to others, nor will I try to use any programs or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.

Signed: _____

Date: _____

## Appendix F: Staff procedure for dealing with an Online Safety Incident



## Appendix G: Procedure for Changes to the Internet Filtering Settings

There is a delicate balance to be struck between legitimate access to websites for educational purposes and protecting pupils against illegal or inappropriate material. There will be occasions where the balance is incorrect and adjustments need to be made.

This procedure sets out how the School will deal with requests for open sites to be blocked or blocked sites to be opened.

Additional blocking or filtering.

Any member of the School community who accesses a site which they believe should be blocked must report it to the IT Support Department as soon as practical, giving the following information:

1. Web address of the site,
2. How they became aware of it, e.g. details of the search that found it,
3. Nature of the concern,
4. Which School device they accessed it from.

The IT Support Department will block the site immediately, before investigating to confirm that the site does, indeed, raise concerns.

If there is any doubt about the appropriateness of the materials, IT Support Staff will consult with the staff involved and/or the The Designated Safeguarding Lead for Child Protection to agree whether it should be blocked. If necessary, the Headmaster will make the final decision.

In the event that it is agreed not to block, the IT Support Department will re-open the site.

The IT Support Department will let the originator of the request know the outcome.

In the event that the site in question contains illegal material, the IT Support Department will report it immediately to the Internet Watch Foundation (http://www.iwf.org.uk/).

Requests for unblocking.

Requests for sites to be unblocked may only be made to the IT Support Department by members of staff.

The IT Support Department requires a minimum of 24 hours notice to consider an unblocking request. It is essential, therefore, that staff planning to use websites as part of a lesson check in advance whether it is accessible through the School network and on the device(s) they intend to use.

Requests for access to a blocked site should include the following information:

1. Web address of the site or particular page to be accessed,
2. Justification for using the site,
3. View on whether the site poses any risks (eg it may be legitimate to request access to a normally-blocked site containing race hate materials if they are essential to a 6th Form lesson but the site may still pose a risk to other pupils),
4. When access is required,
5. Year or group of pupils, and/or staff members who require access,
6. Whether the site should be temporarily or permanently opened.

The IT Support Department will consider the request.

If there is any doubt about the appropriateness of the materials, IT Support Staff will consult with the member of staff concerned and/or the The Designated Safeguarding Lead for Child Protection to agree if it can be opened. If necessary, the Headmaster will make the final decision.

If agreed the IT Support Department will open the site either permanently or temporarily and let the originator of the request know the outcome.

In the event of temporary access, they will schedule the re-blocking of the site at the end of the agreed period.

Recording.

The IT Support Department will maintain a log of all change requests.

**Unblocking of Apps and websites for use by international Boarders**

Boarders will be able to use the School's BYOD network for their devices, for use both during and outside of the normal school day. The School appreciates that its usual filtering and blocking service may not be appropriate due to both the residential and international elements of their relationship with the School. In such a case that a boarder wishes to access a blocked site or App, they can approach their Houseparent who will submit a request to ICT. At the start of each academic year and at regular intervals the Head of Boarding will also survey the boarders to give them the opportunity to suggest Apps and websites which need unblocking, particular priority will be given to Apps and devices which allow for boarders to safely and efficiently contact their friends and relatives back home.

## Appendix H: Guidelines for taking images (photos and videos) of pupils

1. Photographs should only be taken on School owned cameras. These can be borrowed from Reception if you do not have access to one in your own department,
2. Before uploading photographs on to the School network, staff should use the camera to sift through their photographs and delete any that are sub-standard, duplicates etc,
3. Note this is an important step,
4. Photographs are only allowed to be stored on the M: drive of WGS Shared. This drive will only be available in school and on School computers,
5. Note this means it will not be visible via remote access and also not available to pupils,
6. Before transferring photos, a suitably named folder needs to be set up the Upload folder on the M: drive first. The name of the folder should be of the form <date of trip as YYYYMMDD><staff initials><name of activity> e.g. 20150821MLFParis,
7. Photographs should then be transferred from the camera to this folder using a school computer. Please contact the Helpdesk if you need help doing this. The photographs should then be deleted from the camera, and any borrowed cameras should be returned to Reception.

Marketing will then check through new folders in the Upload folder and then copy them into the relevant School Year folder in the Photographs folder. All photos stored here will be accessible by all school staff and can be used in school presentations or other publicity activities. Note that any presentations that are to be shown to parents, prospective parents or groups outside school should be checked with Marketing to ensure consistency.

Please remember staff should not store photographs of pupils on their own personal equipment, including PCs, laptops, tablets, mobile phones, portable drives etc. Similarly, photographs should not be stored on any other drives on the School network. Please note that, periodically, the network will be scanned for photographs; any not stored on the M: drive will be removed and may be deleted. Presentations and documents containing photographs of pupils should only be stored on the school network.

In addition, we request that photos are not uploaded to social media or websites. Requests can be made to Marketing to have photos posted up on the School website and/or the Social Media pages

## Appendix I: Staff guidelines for the potential risk of radicalisation for pupils using social media

This guidance relates to the Government's advice contained in its Prevent Strategy that was published in 2015 and has now become incorporated into the Safeguarding and Child Protection Policy. Staff are advised to be aware that vulnerable people may be at risk of becoming radicalised by extremist groups. A key communication tool which such groups use is social media.

Hence, staff should be vigilant with regard to pupils interacting with extremist groups digitally and ensure that they are reminded of standard Online Safety advice e.g. not to become friends with a stranger and not to post and allow easy access to personal information.

However, if staff become aware of a pupil being influenced in any way by extremist groups (whether through social media or not), this should be raised immediately as a concern with one of the Prevent Lead or a member of the DST

Also note that the School cannot be held accountable for the actions of, content held, or data processed by third parties. With the rise in social media and cloud services it is important to understand the School cannot police or moderate these systems, and can only ever provide guarantees for the systems over which it has direct control.