# E-Safety Policy

## Introduction

Immanuel School endeavours to ensure the e-safety of both pupils and staff. We believe it is important to recognise both the benefits and dangers of technology, seeking to use it wisely and in a way that honours God. Part of our mandate as a school is to 'prepare, disciple and educate young people' to ensure they can deal with 'the opportunities and challenges of a changing world' and, increasingly, this includes teaching and training pupils how to use the Internet and related technologies safely, wisely and productively.

## Development/monitoring/review of the Policy

This e-safety policy has been developed by a working group made up of:

- Immanuel School Principal
- School Management Team
- School Leadership Team
- Safeguarding Lead / Trustee with specific oversight for Immanuel School
- School teaching staff
- I.T specialist/ technical staff (Alex Agrenich, Caleb Cope)

It now incorporates all Filtering & Monitoring (FAM) requirements, which will help the school monitor the impact of the policy, along with the above groups.

## Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers and visitors) who have access to and are users of school ICT systems.

The Education and Inspections Act 2006 empowers Principals to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The school will deal with such incidents within this policy, associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of school.

## Roles and Responsibilities

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

**Trustees/Management:**

These are responsible for the approval of the e-safety policy and for overseeing the review of its effectiveness. FAM procedures, FAM reports and incidents and curriculum issues will be taken in to account.

**Principal:**

The Principal has a duty of care for ensuring the safety (including e-safety) of all members of the school community, working in conjunction with the Safeguarding Lead, who is responsible specifically for FAM. The Principal and Safeguarding Lead should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff (see appendix 3). The Principal and Safeguarding Lead should ensure they have received suitable training to enable them to carry out their e-safety roles and to train other colleagues, as appropriate (see TES/ Educare modules 'Online Safety' and 'Cyber Security').

The Principal will include a summary and review of e-safety in the termly report to the Trustees/ Management, including FAM.

**E-safety Coordination (Principal and Safeguarding Lead):**

Working in tandem, the Principal and Safeguarding Lead will take day to day responsibility for e-safety issues (working with specifically designated staff – see Appendix 6) and will take the leading role in establishing and reviewing the school e-safety policies/documents. As part of this role, they will ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place. They will provide an appropriate level of training and advice for staff. The role also involves liaison with Safeguarding Partners, including the Prevent & Hate Crime Coordinator, where relevant, as well as with school technical staff.

The Principal will monitor use of school email addresses on a regular basis and, along with Safeguarding Lead and technical staff, receive daily reports the FAM system. This will be used to create a log of incidents to inform future e-safety developments. Any sanctions will be imposed by a member of the school leadership team or the Principal (see appendix 2). They will consult with pupils, parents and staff where appropriate. They will map and review the e-safety curriculum provision – ensuring relevance, breadth and progression.

**Teaching Staff:**

Staff are responsible for ensuring that they have an up to date awareness of e-safety matters and of the school's current e-safety policy and practices, including FAM and they will read this policy every September to ensure they are up to date. They will receive annual e-safety training via our online training provider – TES/ EduCare – entitled 'Online Safety' and 'Cyber Security' and sign the Staff Acceptable Use Agreement (AUA) (Appendix 4) - a signed copy of which will be kept in school records.

Although FAM procedures are in place, staff are aware that they must report in writing any suspected misuse or problem to the Principal or Safeguarding Lead for investigation, action and sanction. All digital communications with pupils, parents and carers should be on a professional level and only carried out using official school systems and procedures. They need to ensure that e-safety issues are embedded in all aspects of the curriculum and other activities, and that pupils understand and follow their e-safety contracts. They need to ensure that pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations. They also need to ensure they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices. In lessons where Internet use is pre-planned, pupils should be guided to sites checked as suitable for their use.

In addition, all staff will be expected to do the following:

- Use the Internet and communications technologies wisely and in an appropriate manner.
- Not use computers which are accessible to pupils for personal use – emails, shopping, social networking sites etc.
- Not download programmes onto computers without checking with a member of the leadership team.
- Ensure that all computer screens are easily visible when pupils are using them.
- Report any personal e-safety concerns to the Principal or Safeguarding Lead, as appropriate.
- Know and reinforce e-safety practices with the pupils wherever possible.
- Offer pupils advice and support in the classroom where minor e-safety issues have occurred.
- Report more serious student e-safety concerns to the Principal or Safeguarding Lead as appropriate – although the FAM system will highlight anything that may be missed by staff at the time).

**Pupils:**

Pupils are responsible for using the school's digital technology systems in accordance with their AUA (Appendix 5). They are expected to have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations. They need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so and will be expected to know and understand school policy on the use of images and on cyber-bullying. They should also

understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's e-safety policy covers their actions out of school, if related to their membership of the school. All pupils will be expected to do the following:

- Hand in mobile phones to Form Tutors for the duration of the school day.
- Pay careful attention to e-safety advice.
- Only use the computers/Internet with staff permission.
- Only log on with their own personal passwords.
- Not share personal passwords with anyone.
- Not go on to unsuitable sites, nor access chatrooms, send or receive emails (with the exception of School emails).
- Remember that Internet history and usage is filtered and monitored – which they are informed of.
- Report any e-safety concerns to staff immediately when they occur.
- Not delete inappropriate messages or images from technology until they have been seen by a teacher.
- Sign and outwork their e-safety agreements.
- Use only their school email addresses to send work/information into and out from school computers.
- Use Microsoft teams as directed, on which the messaging facility has been disabled.

**Parents/Carers:**

Parents and carers play a crucial role in ensuring that their children understand the need to use the Internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, informative emails, the school social media platforms and information about national/local e-safety campaigns and literature.

## Educating in e-safety

**Pupils:**

Whilst regulation and technical solutions are very important, our goal is to educate and train pupils to take a responsible approach, recognising and avoiding e-safety risks. The education of pupils in e-safety is therefore an essential part of the school's provision and staff should reinforce e-safety messages.

The school's e-safety curriculum is relevant to the needs of pupils and provides progression; it will be provided in the following ways:

- eSafety is provided as part of Computing, Focus lessons and assemblies and all pupils participate in the annual national *Safer Internet Day.*
- Pupils should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.
- Pupils will be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making. (NB. Immanuel School is aware of the additional duties for schools under the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material on the Internet. See Preventing Radicalisation and Extremism Policy).
- Pupils should be helped to understand the need for the student AUA and encouraged to adopt safe and responsible use both within and outside school.
- Where pupils are allowed to freely search the Internet, staff will be vigilant in monitoring the content of the websites the pupils visit.
- It is accepted that, from time to time, for good educational reasons, pupils may need to research topics (eg racism, drugs, discrimination) that would normally result in Internet searches being blocked. In such a situation, staff (under guidance from the Safeguarding Lead/ Leadership Team) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be justified with clear reasons.
- Pupils will be given training to ensure that they know how to mitigate against e-safety risks by using safe practices whilst online.
- Education and training will be provided by the school to ensure that pupils know when, how and to whom, to report instances when their e-safety may have been compromised.
- Education and training will seek to reassure pupils that they are in an environment that encourages them to report e-safety issues without risk of reprimand, humiliation or embarrassment.

**Staff:**

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- E-safety training will form a significant part of ongoing internal training for all staff.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreement.

- The Principal and Safeguarding Lead will receive regular updates through attendance at external training events (eg from SWGfL / LA / other relevant organisations) and/or by reviewing guidance documents released by relevant organisations.
- Staff will receive advice/guidance/training as required.
- Ex-staff will be removed from email and One Drive on a termly basis.

**Parents/carers:**

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of their children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the Internet and may be unsure about how to respond.

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

- Emails, content on the Immanuel School web site
- Parents' evenings
- Events/campaigns e.g. Safer Internet Day

Parents are annually informed about our FAM procedures.

## Technical- Equipment, Filtering and Monitoring

The school will be responsible for ensuring that the school equipment/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. A significant part of this is our FAM system. The school will also ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities. Staff with specific roles with regard to FAM are listed in Appendix 6.

- All users will have clearly defined access rights to school systems and devices.
- All senior pupils will be given an email account for use when sending work/information to and from school. Personal email addresses must not be used for this purpose. Regular checks will be carried out to monitor the use of emails by all senior pupils by the Principal.
- All users (at KS2 and above) will be provided with a username and secure password. Up to date records of users and their usernames will be stored by technical staff. Users are responsible for the security of their username and password and will be required to change their password when requested by the Leadership team.

- Ben Cope (Safeguarding Lead) is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all computers accessed by pupils, except for those in room 7 where it is not independently used by pupils. PCs in room 3, pupil laptops and any staff devices linked to the Hall and upper corridor WI-FI are both filtered & monitored by the Smoothwall FAM system.
- The Principal and/or Safeguarding Lead will be informed if there is a report of any actual/potential technical incident/security breach.
- Daily alerts are generated for the Principal, Safeguarding Lead and technical staff, which are then handled accordingly – including no action, disciplinary or safeguarding measures. Responses to alerts will be within 24 hours (or Monday if generated over the weekend).
- Staff may not download executable files or install programmes on school devices without express permission granted by the Principal or member of the Leadership Team.
- An annual FAM audit and risk assessment will be carried out by the Safeguarding Lead, in conjunction with the principal, Management Team and technical staff, which will be agreed by the trustees.
- A full list of roles and responsibilities is stored in the FAM/ eSafety folder, in the Safeguarding Lead's office.

## Cyber Security and Artificial Intelligence (A.I)

Immanuel recognises that technology is developing exponentially, but commits to remaining as up to date as is reasonably possible. Technical staff will undergo annual training and disseminate information to all staff, as appropriate.

Immanuel adheres to Cyber Security standards for Schools and Colleges published by the DfE, which are referred to in KCSIE 2024 and are a key factor in our approach to eSafety.

Further detail about Cyber Security is in the **Immanuel Cyber Security Plan**, which is reviewed annually.

As stated in their AUAs, pupils are prohibited from using A.I unless given specific permission to do so and staff need to remain vigilant in this area.

## SOME USEFUL CONTACTS & DOCUMENTS

- DfE: Teaching E-safety in Schools – updated January 2023 - https://www.gov.uk/government/publications/teaching-online-safety-in-schools
- UKCIS e-safety in schools & colleges governing board https://www.gov.uk/government/publications/online-safety-in-schools-and-colleges-questions-from-the-governing-board
- CEOP (Child Exploitation and Online Protection Command) https://www.ceop.police.uk/Safety-Centre/
- LGfL https://national.lgfl.net/home/about-us

## USE OF COMMUNICATION TECHNOLOGIES

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how Immanuel School currently considers the benefit of using these technologies for education outweighs their risks/disadvantages:

| Communication Technologies | ***Staff*** | | | ***Pupils*** | | | | |
|---|---|---|---|---|---|---|---|---|
| | Allowed | Allowed at certain times | Allowed for selected staff | Not allowed | Allowed | Allowed at certain times | Allowed with staff permission | |
| Mobile phones may be brought to the school | X | | | | X | | | |
| Use of mobile phones in lessons | X | | | | | | X | |
| Use of mobile phones in social time | X | | | X | | | | |
| Taking photos on mobile phones / cameras | | | X | | | | X | |
| Use of other mobile devices e.g. tablets, gaming devices | X | | | X | | | | |
| Use of personal email addresses in school / academy , or on school / academy network | | | X | X | | | | |
| Use of school email for personal emails | X | | | N/A | | | | |
| Use of messaging apps | X | | | X | | | | |
| Use of social media | | | X | X | | | | |
| Use of blogs | X | | | | | | X | |

## DEFINITION OF MISUSE

Issues related to the misuse of the Internet and associated technologies will be considered and dealt with in line with the discipline, bullying and safeguarding policies. At Immanuel School, the following criteria apply for all Internet and technology users in relation to what is unacceptable use:

| User Actions | Acceptable | Acceptable at certain times | Acceptable for nominated | Unacceptable | Unacceptable and illegal |
|---|---|---|---|---|---|
| Using school systems to run a private business | | | | X | |
| Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy | | | | X | |
| Infringing copyright | | | | X | |
| Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords) | | | | X | |
| Creating or propagating computer viruses or other harmful files | | | | X | |
| Unfair usage (downloading / uploading large files that hinders others in their use of the Internet) | | | | X | |
| On-line gaming (educational) | | X | | | |
| On-line gaming (non-educational) | | X | | | |
| On-line gambling | | | | X | |
| On-line shopping / commerce | | | x | | |
| File sharing | | X | | | |
| Use of social media | | | X | | |
| Use of messaging apps | | | X | | |
| Use of video broadcasting e.g. Youtube | | X | | | |

Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

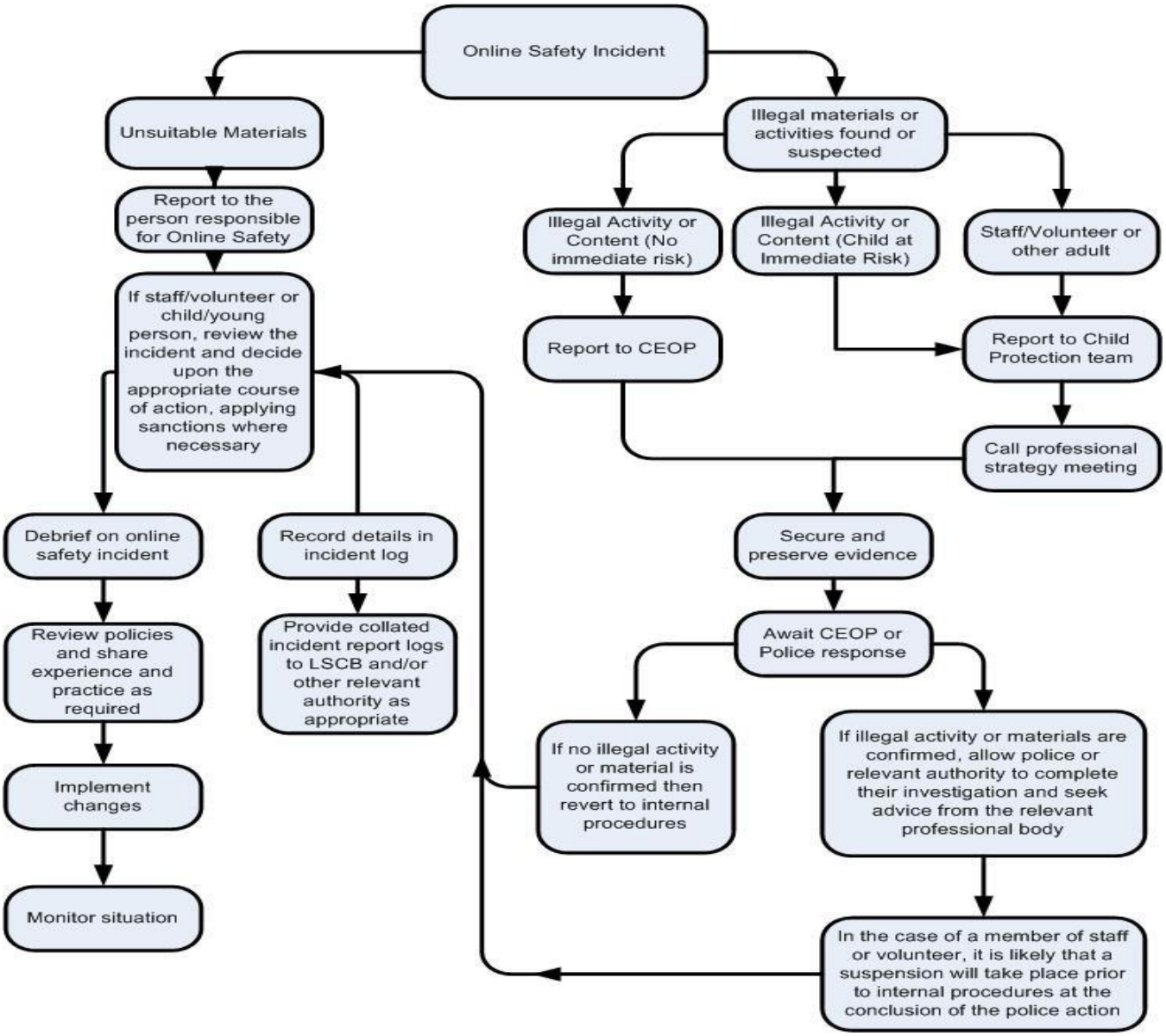
- Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978

- Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.
- Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008
- Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986
- Pornography
- Promotion of any kind of discrimination
- threatening behaviour, including promotion of physical violence or mental harm
- Promotion of extremism or terrorism
- Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. Where these incidences occur, it is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with in accordance with the school discipline policy and procedures.

## APPENDIX 1 : SUMMARY OF GUIDANCE WHEN HANDLING AN E-SAFETY INCIDENT

This flow chart can be used as guidance to help any member of staff in handling an incident. Where it is uncertain who to report to, the Principal will be the point of contact as DSL. If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below) for responding to e-safety incidents and report immediately to the police.




**CEOP (Child Exploitation and Online Protection)**

**LSCB (Local Safeguarding Children Board – now 'Partners')**

## APPENDIX 2 : SUMMARY OF SANCTIONS FOR PUPILS

**Pupils** **Sanctions/actions**

| Incidents: | Refer to Principal | Refer to Head of Department / Head of Year / other | Refer to Headteacher / Principal | Refer to Police | Refer to technical support staff for action re filtering / security etc | Inform parents / carers | Removal of network / Internet access rights | Warning | Further sanction eg detention / |
|---|---|---|---|---|---|---|---|---|---|
| **Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).** | X | X | X | X | X | X | X | | X |
| Unauthorised use of non-educational sites during lessons | X | | | | | | | | |
| Unauthorised use of mobile phone / digital camera / other mobile device | X | | | | X | X | | | |
| Unauthorised use of social media / messaging apps / personal email | X | | | | X | X | | | |
| Unauthorised downloading or uploading of files | X | | | | X | X | | | |
| Allowing others to access school network by sharing username and passwords | X | | | | X | X | | | |
| Attempting to access or accessing the school network, using another student's / pupil's account | X | | | | X | X | | | |
| Attempting to access or accessing the school network, using the account of a member of staff | X | | | X | X | X | | | X |
| Corrupting or destroying the data of other users | X | | | X | X | X | | | X |
| Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature | X | | | X | X | X | | | X |
| Continued infringements of the above, following previous warnings or sanctions | X | | | X | X | X | | | X |
| Actions which could bring the school into disrepute or breach the integrity of the ethos of the school | X | | | X | X | X | | | X |
| Using proxy sites or other means to subvert the school's filtering system | X | | | X | X | X | | | X |
| Accidentally accessing offensive or pornographic material and failing to report the incident | X | | | X | X | X | | | |
| Deliberately accessing or trying to access offensive or pornographic material | X | | | X | X | X | | | X |
| Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act | X | | | X | X | X | | | |

## APPENDIX 3 : SUMMARY OF SANCTIONS FOR STAFF

Staff Sanctions/actions

| Incidents: | Refer to line managerr | Refer to Headteacher Principal | Refer to Police | Refer to Technical Support Staff for action re filtering etc | Suspension | Disciplinary action |
|---|---|---|---|---|---|---|
| **Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).** | | X | X | | | |
| Inappropriate personal use of the Internet / social media / personal email | X | X | | | | |
| Unauthorised downloading or uploading of files | X | X | | | | |
| Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account | X | X | | | | |
| Careless use of personal data eg holding or transferring data in an insecure manner | X | X | | | | |
| Deliberate actions to breach data protection rules | X | X | | | | |
| Corrupting or destroying the data of other users or causing deliberate damage to hardware or software | X | X | | | | |
| Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature | X | X | | | X | |
| Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils / pupils | X | X | | | | |
| Actions which could compromise the staff member's professional standing | X | X | | | | |
| Actions which could bring the school into disrepute or breach the integrity of the ethos of the school | X | X | | | | |
| Accidentally accessing offensive or pornographic material and failing to report the incident | X | X | | | | |
| Deliberately accessing or trying to access offensive or pornographic material | X | X | | | X | |
| Breaching copyright or licensing regulations | X | X | | | | |
| Continued infringements of the above, following previous warnings or sanctions | X | X | | | X | X |

**APPENDIX 4:**

# Immanuel School online safety Acceptable Use Agreement – Staff

The following guidelines are to be adhered to by all school staff in order to promote e-safety within the school. Some of the points refer to activities or technology uses that would be appropriate outside of a school setting. However, this document lays out the uses that we deem to be appropriate within a setting where children are co-users of technology.

1. Use the internet and communications technologies wisely and in an appropriate manner
2. Do not use computers which are accessible to students for personal use – emails, shopping, social networking sites etc.
3. Do not download programmes onto a school computer without checking with the relevant member of leadership team.
4. Ensure that all computer screens are easily visible when students are using the computers
5. Report any personal online safety concerns to the Principal or Safeguarding Lead, as appropriate
6. Know and reinforce online safety practices with the students wherever possible
7. If you use Microsoft Teams, ensure that feedback and other communication between you and individual pupils is appropriate and necessary. Also, be aware that parents are encouraged to monitor teacher feedback given to their son(s) and daughter(s).
8. Offer students advice and support in the classroom where minor e-safety issues have occurred
9. Report more serious student online safety concerns to the Principal or Safeguarding Lead as appropriate, who will update the ICT Oversight Folder.
10. Ensure that any private social networking sites/blogs etc that you create or actively contribute to are not confused with your professional role.
11. Ensure any confidential data that you wish to transport from one location to another is protected by encryption and that you follow school data security protocols when using such data.
12. Ensure all documents, data, etc. are saved, accessed and deleted in accordance with the school's network and data security and confidentiality protocols.

Signed: Date:

**APPENDIX 5:**

# Immanuel School online safety Acceptable Use Agreement – Pupils

The following guidelines are to be followed at all times when using computers, laptops and other internet-related technology in school. This will enable students and staff to stay safe and protected. Failure to adhere to the following guidelines may result in removal of access to technology or alternative disciplinary measures.

1. Hand in mobile phones to Form Tutors for the duration of the school day
2. Pay careful attention to online safety advice
3. Only use the computers/internet with staff permission and supervision
4. Do not eat or drink around computers
5. Only log on with your own personal password
6. Do not share personal passwords with anyone
7. Do not go on to unsuitable websites, or access chatrooms
8. Internet and email history for all students will be checked regularly – do not delete your history
9. Report any online safety concerns or incidents to staff immediately they occur
10. Do not delete inappropriate messages or images from technology until a teacher has seen them
11. Do not download any programs to your computer without permission
12. If you have a personal USB at school, ensure it contains only information relevant to your school work
13. All communication on Teams should be related to your school work.
14. All email communication must be appropriate, within school context and only using school provided email accounts.
15. Pupils will NOT access any form of social media or personal email accounts on school computers.
16. Use of AI is prohibited, unless given specific permission to do so.
17. Every September, sign and outwork your e-safety acceptable user agreement

Print Name: Signed: Date:

**APPENDIX 6**

# eSafety Policy – Roles & Responsibilities

| Role | Responsibility | When |
|---|---|---|
| Update eSafety policy | BC | Annually (April) |
| Keep logs of reported e-incidents and alerts/ actions | AA/CC | When alerts arise |
| Monitor FAM system and deal with issues as alerts arise | BC & SW receive alerts<br>AA and CC investigate and feedback | By the end of the school day when the alert arises, or first thing the next day if the alert came too late in the day. |
| Be familiar with eSafety Policy and Appendices – keeping copies in Staff Handbook or electronically. | All<br>(especially Principal & DSL – including AA, CC and LM | Annually (September) |
| Undertake training to carry out e-safety roles and train/ facilitate the training of others | AA – ongoing log of Smoothwall contact<br>BC/ CC - Smoothwall<br>ALL – TES/ EduCare modules | Annually (and as appropriate) |
| Include a summary and review of e-safety in the termly report to the Trustees/ Management. | SW | January, May, September (as Trustees meet) |
| Monitor and report misuse of school email addresses to the Principal | SW – kept in her folder and also BC's eSafety folder | Every 10 days |
| Enforce discipline/ sanctions for e-misconduct | SW, Leadership Team – involving pupils, staff and parents as appropriate | As required |

| | | |
|---|---|---|
| Map and review the e-safety curriculum provision – ensuring relevance, breadth and progression. | SW (with AA and LG) | Annually (July or as required) |
| Ensure a planned e-safety curriculum is provided as part of Computing and Focus lessons, as well as assemblies eg: safer Internet Day | SW (with AA and LG) | Annually (July or as required) |
| Store up to date records of users and their usernames | AA | Annually (and as appropriate) |
| Ensure the security of usernames and passwords and change these when requested by the Leadership team. | All | Annually (and as appropriate) |
| Ensure software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations. | AA (including BC as appropriate) | Annually |