Ras Al Khaimah American Academy				
Subject: Reporting Policy			**SOP No:**	**Controlled Copy No:**
			Revision No: New	
Written by:	**Online Safety Lead Assistant**	**Date:**	**Policy based on:**	
	Ms. Katrina Scotford	19/04/22		
Checked by:	**ICT Manager**	**Date:**	**Supersedes: New**	**Issued on: 22/04/22**
	Ms. Asma Odawa	21 May 2022		
Approved by:	**Principal**	**Date:**	**Distributed to:**	**Pages: 6**
	Dr. Sandra Zaher	22/04/22		
Authorized by:	**Principal**	**Date:**	**Policy effective as of: 22/04/22**	
		22/04/22	**Policy review date: September 2022**	

Contents

Introduction

As Acceptable Use Policies are updated to reflect the fast-moving changes in education as a result of the COVID-19 pandemic so too must the methods of reporting any breaches of the AUP by staff members, students, their parents, and other members of the RAKAA community. The ways in which issues are reported need to be updated to reflect the times we are living in and an online record must be kept to help establish any patterns or links and allow for an audit to identify problems and patterns.

Rationale

The purpose of this policy is to lay out the methods of reporting for all stakeholders at RAKAA with regard to online safety issues. In order for reporting to be effective, it must be transparent and easy to follow with a clear method for all stakeholders to access.

If a breach of any AUP has been identified, then users within the RAKAA community have a duty to report it to the IT department and the Online Safety Group to be investigated.

Students

Any student who suspects a breach of the AUP or who may find that they have accessed any content that concerns them should in the first instance report the concerns to either their Homeroom Teacher, their class teacher or the IT department to be investigated.

We do recognize that some students may not feel confident in reporting issues to their teachers for fears of reprisals and so we have produced a set of posters to be displayed in all Homeroom classes and enlarged and shared prominently around the school in common areas.

The students will be able to scan a QR code that has been inserted on the posters and they will be directed to a Microsoft Form https://forms.office.com/r/zkZAiEmgSE on which they can select which category their concern falls under and fill in all relevant information which will then be submitted to the IT department to be recorded before being forwarded to the Online Safety Leader to determine the outcome of the investigation.

Staff

Any staff member who suspects a breach of the AUP or who may find that they have accessed any content that concerns them should in the first instance report the concerns to the IT department to be investigated.

The staff members will be able to scan a QR code that has been inserted on a poster that will be emailed to all staff and distributed via paper copy and they will be directed to a dedicated Microsoft Form https://forms.office.com/r/bhW2thQhAb on which they can select which category their concern falls under and fill in all relevant information. Staff members also have the option to upload any evidence of their concerns or breaches. Once completed, their response will then be submitted to the IT department to be recorded before being forwarded to the Online Safety Leader to determine the outcome of the investigation.

Parents

Any parents who suspect a breach of the AUP can also notify the school via a dedicated QR code and link to a Microsoft Form https://forms.office.com/r/zkZAiEmgSE As with the students and staff, Parents will have a dedicated poster that Homeroom teachers will post to their Microsoft Teams platforms for Parents to access.

Following the protocol for students and staff, the form for parent AUP concerns will be delivered to the IT department in the first instance before being forwarded to the Online Safety Leader to investigate and determine any outcomes.
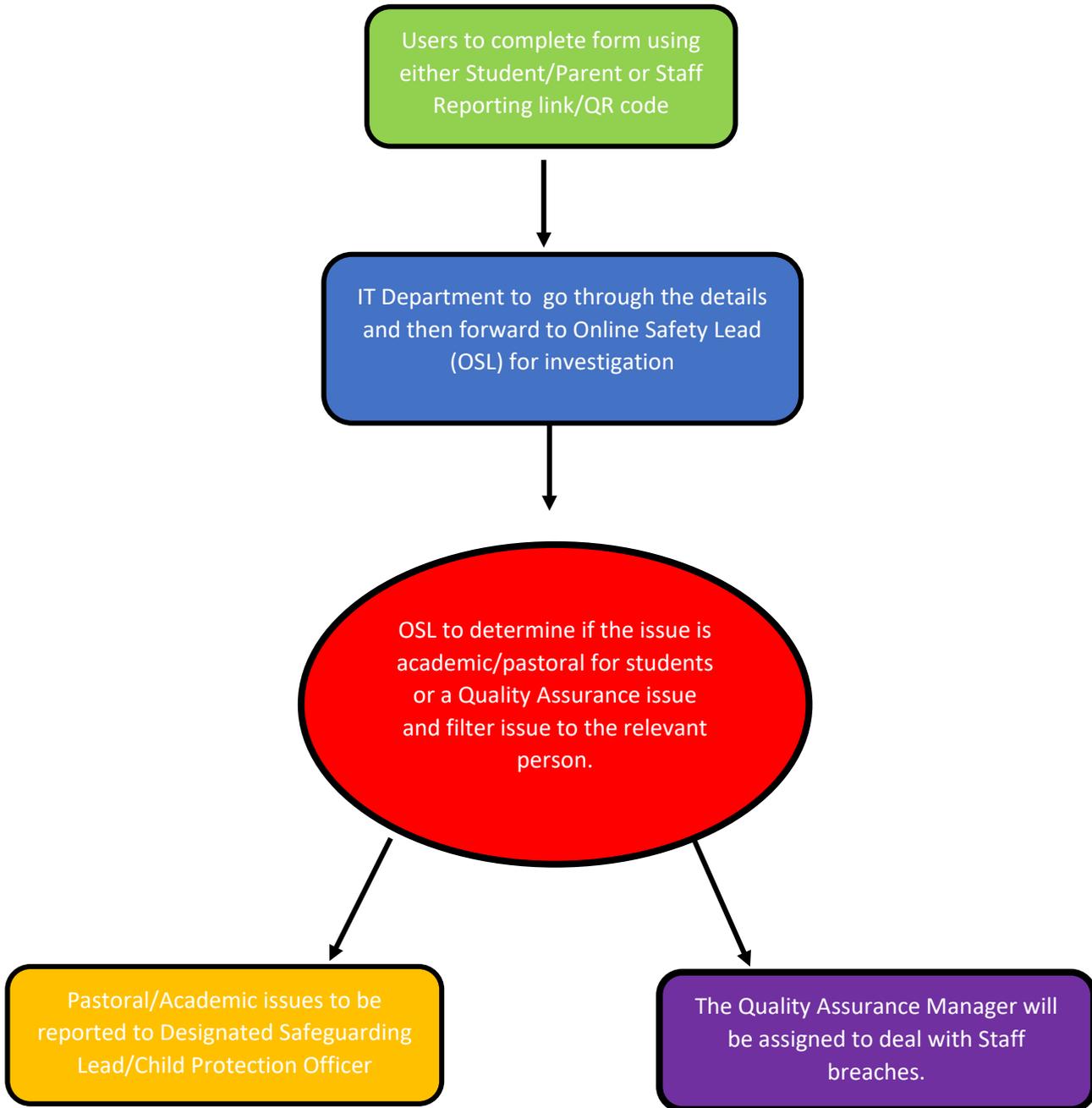
School website

The individual links for students and parents to report any issues will also be added to the school's website so any member of the school community can report any E-Safety issues with ease.

Factors Considered by RAKAA:

- We consider these Procedures for incidents audits records as senior, moderate, and minor to match with every incident and designated consequences
- The school is reviewing and analysing data of incidents reports once per
- The school considers date reviewed report to ensure implementation and links to online safety policy
- If a teacher reported that he/she lost an important document, which was created through office 365 they inform IT department and we recover the file.
- In the AUP stakeholders are informed that when facing any technical issues they need to contact IT.

- Also same was informed to staff through trainings and parents were informed through messages and students dairies about how to contact IT
- The school is using phenomenal for administrative consultancy to consult with, when it comes to online safety incidents as a local expert

Reporting protocol

```
┌─────────────────────────────┐
│ Users to complete form using│
│ either Student/Parent or Staff│
│ Reporting link/QR code      │
└─────────────────────────────┘
              │
              ▼
┌─────────────────────────────┐
│ IT Department to go through │
│ the details and then forward│
│ to Online Safety Lead       │
│ (OSL) for investigation     │
└─────────────────────────────┘
              │
              ▼
     ┌─────────────────────┐
     │ OSL to determine if │
     │ the issue is        │
     │ academic/pastoral   │
     │ for students or a   │
     │ Quality Assurance   │
     │ issue and filter    │
     │ issue to the        │
     │ relevant person.    │
     └─────────────────────┘
       │                 │
       ▼                 ▼
```

Pastoral/Academic issues to be reported to Designated Safeguarding Lead/Child Protection Officer

The Quality Assurance Manager will be assigned to deal with Staff breaches.

Reporting of technical issues

Staff, students and parents can contact the IT department using any of the below channels to report technical issues:

1. IT Support email: itsupport@rakaag.com
2. Microsoft Teams: a.odaw@rakaa.sch.ae, n.ahmad@rakaa.sch.ae
3. IT WhatsApp support: 0565005356., 0562535667

Outside Agencies

In order to fully ensure the safety, security and well-being of our students and other stakeholders at RAKAA, we ensure that all of our practices follow guidelines that have been provided by the Ministry of Education and we integrate them into our systems.

These guidelines are followed in our Child Protection Policy, Behavior Policy, Cyberbullying and Anti-bullying policies as well as our Acceptable Use policies and we also follow the sanctions as prescribed by the MoE.

RAKAA is aware of the MoE's Child Protection Unit and its purpose in implementing the measures and mechanisms of child protection within educational settings as stipulated by Federal Law No. 3 2016 (Wadeema's Law) and it's executive regulations. The purpose of the 'Child Protection Unit' launched by the MoE is to ensure that students at government and private schools within the UAE are protected from all forms of harm, neglect or abuse whether in an educational setting or at home in order to maintain their safety as it relates to their physical, educational or psychological development.

At RAKAA we encourage all members of our community to be vigilant when online both on campus and when at home. If anyone feels they need further support with any Digital or E-Safety issues not associated with RAKAA then we urge them to call 80091 to access the UAE Digital Wellbeing Support Line (for Arabic Speakers) which is the recognized as the first initiative of the Digital Wellbeing Council. Callers to this support line will be given professional advice from key experts within the Digital community that is tailored to their situation and covers practical situations that users may find themselves in whilst online.

In its drive to be a world leader in E-Safety, the UAE has placed a serious focus on Cybersafety and digital security.

Report cybercrimes online

If a parent, member of staff or student believes that they have been a victim of cybercrime then we encourage them to use the following links and channels in order to report it to the relevant authorities:

- The eCrime website - https://www.dubaipolice.gov.ae/wps/portal/home/services/individualservicescontent/cybercrime
- Dubai Police's website - https://www.dubaipolice.gov.ae/wps/portal/home/services/institutionsservices/cybercrimeService/!ut/p/z1/04_Sj9CPykssy0xPLMnMz0vMAfIjo8zi_T29HQ2NvA183U19DQwc3Vwc3U3MXYwNLlz1w1EV-JsFmxg4mhqbuVgYmRsaeJrrRxGj3wAHcDQgrD8KTYm3m6GBo4-niXlYoImBga8hugI0JwYSUgDyA1gBHkcGp-bpF-SGRhhkeuoCAASrB98!/p0/IZ7_P9K01802MGGK30Q8TCLJCD20A2=CZ6_OIKA12K0MG5M00AFDAG47D3083=LA0=Eaction!serviceAction==/#Z7_P9K01802MGGK30Q8TCLJCD20A2
- The 'My Safe Society' app which was launched by the UAE's federal Public prosecution (the app is available on iTunes or Google Play)

Related links:

- Reporting prohibited content to the Internet Service Providers in UAE ;

https://www.tra.gov.ae/en/about-tra/information-and-egovernment-sector/internet-guidelines/details.aspx#description

- Cyber safety and digital security in UAE LAW:

https://u.ae/en/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security

- Digital wellbeing support line http://wam.ae/ar/details/1395302823342

Cross References

The following policies are also linked to RAKAA's Reporting Policy

- Acceptable Use policy (Students, Staff and Outside Agencies)
- Cyberbullying Policy

- Child Protection Policy
- Anti-bullying Policy
- MoE Student behaviour Management – Distance Learning Policy
- Mobile Device Policy
- Online Behavior Policy